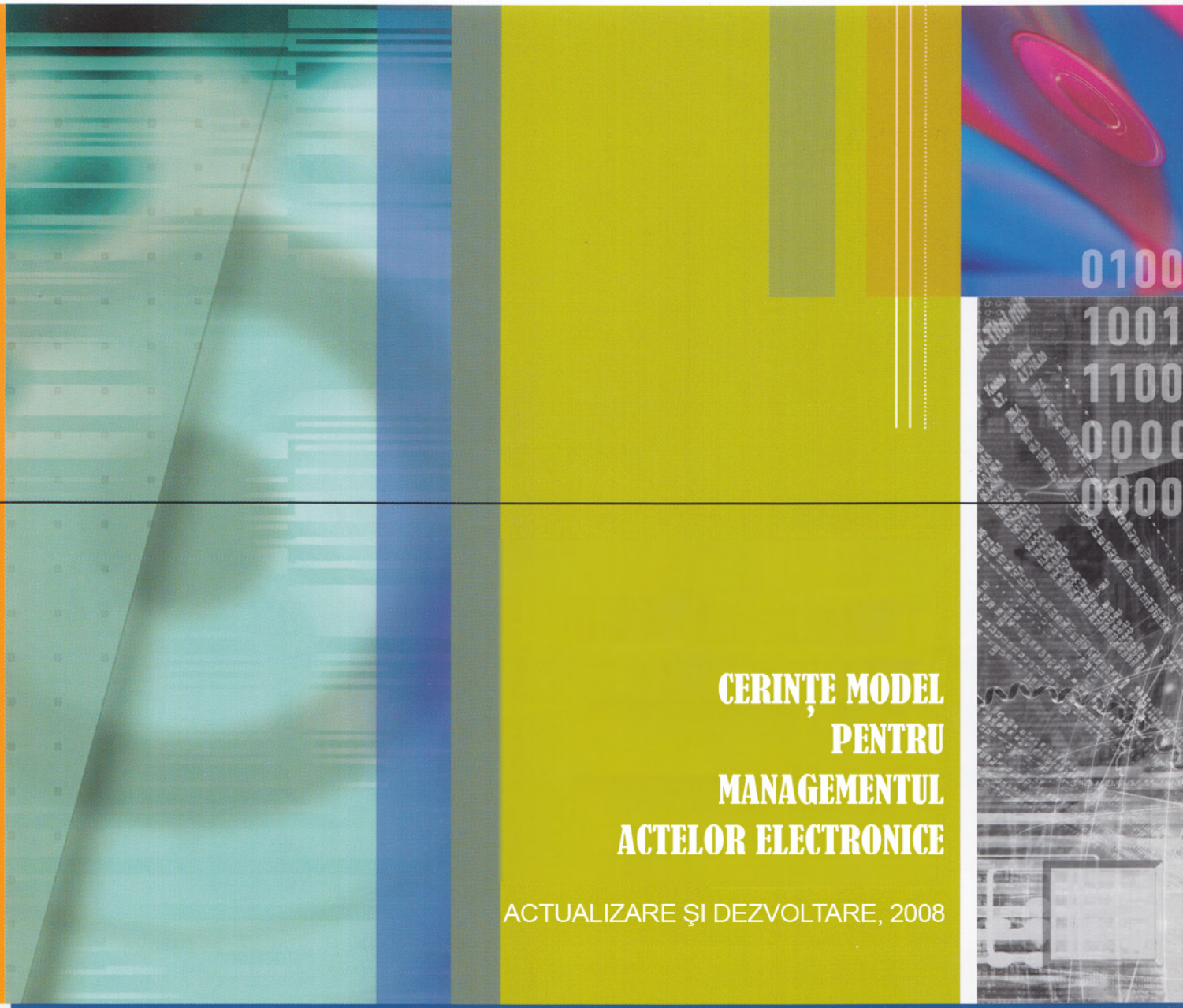
ISBN 978-973-0-12530-6

MoReq2



CERINȚE MODEL PENTRU MANAGEMENTUL ACTELOR ELECTRONICE

ACTUALIZARE ŞI DEZVOLTARE, 2008

SPECIFICAȚIA MoReq 2

COMISIA EUROPEANĂ

DLM-FORUM
Electronic Records

Specificația a fost pregătită de Serco Consulting pentru Comisia Europeană, cu finanțare din partea programului IDABC

Pagină lăsată intenționat albă

COMISIA EUROPEANĂ

MoReq 2 — CERINȚE MODEL
PENTRU MANAGEMENTUL ACTELOR ELECTRONICE

Actualizare şi dezvoltare, 2008

Traducere: Bogdan-Florin Popovici

Brașov

2012

MoReq2 – CERINTE MODEL PENTRU MANAGEMENTUL ACTELOR ELECTRONICE.

Actualizare şi Dezvoltare 2008

(ediția online în limba română)

ISBN 978-973-0-12530-6

Lucrare editată de Federația Arhiviștilor din România

Textul MoReq2 din prezenta ediție a fost aprobat de MoReq Governance Board ca traducere validată în limba română (validator: Lucia Ștefan)

INTRODUCERE LA EDIȚIA ÎN LIMBA ROMÂNĂ

MoReq2 — UN COPIL NĂSCUT BĂTRÂN

Acest text reprezintă o introducere la versiunea în limba română a setului de cerințe model pentru un sistem de administrare a actelor electronice — MoReq2. Prezenta introducere nu reprezintă „chapter zero", așa cum este definit de MoReq2, ci își propune să ofere cititorului român o imagine generală asupra contextului realizării acestui set de cerințe și să justifice o serie de opțiuni de traducere a terminologiei profesionale.

a). Sisteme pentru documente și acte electronice

În evoluția computerelor, a existat un moment de trecere de la faza pur tehnică la etapa „democratizării" producerii de documente digitale, stocate în mediul digital. Din acel moment, producția de documente digitale (fie ele native sau digitalizate) a explodat și, adăugându-se cantităților de documente electronice produse în perioada anterioară, a *mainframe*-urilor, a generat acut nevoia de administrare a acestor documente. Rațiunea era evidentă: dacă în lumea fizică existau dosare, cutii, dulapuri și rafturi, pentru spațiul digital trebuia creat ceva echivalent, care să asigure o ordine pentru documentele care nu puteau fi manipulate fizic[1]. Atunci au început să apară sistemele electronice[2] de administrare a documentelor[3] (*electronic document management system* sau EDMS). Această dezvoltare este stabilită, de diferite surse, la nivelul anilor 1980[4] (cel puțin într-o formă incipientă).

Într-o manieră similară mediului fizic, și în spațiul virtual documentele se clasifică, din punctul de vedere al organizării informației, în două categorii: structurate și nestructurate. Documentele structurate sunt bazele de date și, în lumea fizică, registrele. Documentele nestructurate sunt celelalte… Documentele electronice nestructurate cuprind așadar fișiere generate de aplicații de birou (d.ex., Microsoft Office), fișiere tip imagine, audio, video, pdf sau conținut web[5]. Domeniul EDMS este acela al administrării documentelor electronice nestructurate, asupra cărora efectuează o serie de operațiuni. Odată ce sistemele au devenit mai complexe, aceste operațiuni au devenit tot mai rafinate. Dacă inițial o persoană asigura crearea,

---

[1] Leonard Johnson, *8 Things that Changed the History of Document Management* la http://aiim.typepad.com/aiim_blog/2009/08/8-things-that-changed-the-history-of-document-management.html (toate resursele de pe internet citate în această introducere au fost consultate în data de 5.08.2012).

[2] Deși termenul „electronic" se referă la o gamă larga de dispozitive și documente produse, în acest material vom folosi termenul ca sinonim pentru „digital".

[3] Precizăm că, deși la nivel de masă se consideră tot mai mult că *document management systems* se referă la implicit la documente electronice, în realitate termenul acoperă toate „tehnicile care asigură că o informație înscrisă pe un suport, indiferent de formatul acesteia, este răspândită, folosită, depozitată, regăsită, păstrată, protejată și păstrată de o manieră corespunzătoare, în conformitate cu politici și proceduri stabilite" (Richard Pearce-Moses, *A Glossary of Archival and Records Terminology*, Chicago, 2005, sub voce).

[4] L. Johnson, *loc. cit.*; *Wikipedia*, *sub voce*. (http://en.wikipedia.org/wiki/Document_management_system).

[5] Todd Johnson, *Getting started with document management. Cut costs and boost productivity with a smart document management system* la http://www.networkworld.com/columnists/2011/061411-talking-tech.html. De remarcat că distincția nu este întotdeauna clară, de vreme ce, de pildă, fișierele *.pst generate de MS Outlook au o structură similară unei baze de date, iar o pagină web, de asemenea, poate avea conținutul generat dintr-o bază de date.

denumirea și depozitarea/stocarea documentelor[6], ulterior sistemele au asigurat digitalizarea, captura și indexarea documentelor, stocarea și furnizarea accesului multiplu, securizat[7]. Astăzi, sistemele complexe asigură o multitudine de funcții, cum ar fi:

- captura (prin digitalizare sau luarea sub control a documentelor nativ digitale);
- atribuirea de metadate documentelor precum și indexarea și clasificarea conținutului acestora;
- versionarea documentelor;
- stocarea documentelor și administrarea sistemelor de stocare, inclusiv securizarea acestora împotriva accesului neautorizat;
- acțiuni de căutare și regăsire, pe baza conținutului și a metadatelor;
- operațiuni de editare în vederea publicării, de reproducere în diferite formate și de difuzare a conținutului documentelor.

În plus, sistemele actuale pot furniza o strânsă integrare cu alte aplicații specifice, asigură fluxuri de lucru (creare-aprobare-publicare) și posibilități de lucru colaborativ[8].

Cu ocazia primului Război din Golf (1990–1991)[9], s-a constatat că există o nevoie suplimentară în managementul documentelor, neacoperită de sistemele existente până atunci: administrarea actelor (records management)[10]. Mai multe surse[11] indică faptul că, în urma unei anchete a unei Comisii a Congresului SUA referitoare la Sindromul Golfului, Ministerul (Departamentul) Apărării nu a reușit să furnizeze actele solicitate de investigatori. „Congresul a concluzionat că Ministerul (Departamentul) Apărării nu a reușit să își administreze actele [electronice] și, în consecință, multe dintre actele necesare au fost distruse sau pierdute. Congresul a cerut atunci Ministerului (Departamentului) Apărării să își îmbunătățească capabilitățile de administrare a actelor”[12]. În cooperare cu National Archives and Recods Administration au fost elaborate un raport, apoi un set de cerințe pentru aplicațiile de administrare a actelor electronice, reunite în 1997 sub denumirea DoD 5015.2. „DoD 5015.2-STD a marcat începutul tranziției de la sistemele tradiționale la sistemele digitale în administrarea actelor. DoD 5015.2-STD a făcut posibil transferul responsabilităților de administrare a actelor de la arhivă la birourile de producție, din mâinile câtorva, puțini, practic în mâinile tuturor angajaților”[13].

Schimbări evolutive și revoluționare…[14]

Înainte de DoD 5015.2-STD

- documentele native digitale trebuiau printate înainte de a fi arhivate (administrate ca acte)
- mesajele electronice nu puteau fi stocate în formatele lor native, nici nu se putea confirma integritatea acestora.
- abia dacă exista vreo aplicație comercială care permitea îndeplinirea tuturor funcțiilor necesare pentru administrarea actelor electronice.
- doar arhiviștii pregătiți declarau și clasificau actele.
- Sistemele de administrare a actelor erau limitate la urmărirea actelor pe hârtie

[6] L. Johnson, loc. cit.
[7] T. Johnson, loc. cit.
[8] Wikipedia, http://en.wikipedia.org/wiki/Document_management_system.
[9] Marc Fresko, *MoReq. What do we do now?*, 2010, p. 3 la http://www.intellectuk.org/index.php?option=com_docman&task=doc_view&gid=4748&Itemid=102.
[10] Pentru justificarea traducerii *record* = act vezi partea a doua a prezentului material.
[11] M. Fresko, *loc. cit*.; idem, *MoReq2 and how to use it*, prezentare la Conferința DLM Forum de la Toulouse, 2008; *DoD 5015.2-STD - What's the Big Deal?* la http://jitc.fhu.disa.mil/cgi/rma/dod50152bigdeal.aspx.
[12] *Ibidem.*
[13] *Ibidem.*
[14] *Ibidem.*

- Sistemele de administrare a actelor nu erau legate de informațiile organizației și structura tehnologică
- Administrarea mesajelor vocale, a documentelor web și a mesageriei instantanee ca acte era ceva de neînchipuit.

După DoD 5015.2-STD:

- sistemele de administrare a actelor electronice au devenit parte a infrastructurii tehnologice a organizației
- managementul actelor electronice a devenit o parte integrantă în proiectarea și dezvoltarea aplicațiilor și sistemelor informatice de activitate
- persoana cea mai calificată să stabilească scopul pentru activitate și folosirea actelor devine responsabilă pentru declararea și clasificarea actelor

În mod obișnuit, un ERMS îndeplinește o serie de funcții esențiale din perspectiva managementului actelor electronice. Astfel, captura unui document este similară înregistrării unui act pe hârtie la registratură. După momentul capturii, un document devine act, adică este luat în administrare oficială de organizația respectivă; asupra lui nu se pot efectua nici un fel de modificări și nici actul nu trebuie să poată suferi schimbări, indiferent de tehnologia de citire/vizualizare — devine static. În acest sens, orice acțiune care are ca subiect respectivul act trebuie urmărită și înregistrată într-o evidență de auditare. Mai departe, actul este „clasificat”[15] într-o categorie (clasă) prestabilită printr-o schemă de clasificare a actelor. Aceasta, similară nomenclatorului arhivistic, stabilește contextul actului respectiv și implică și atribuirea unui termen de păstrare. În cadrul clasei, actul poate fi plasat într-un dosar — de o manieră similară sistemului fizic, alături de alte acte pendinte aceleiași activități, persoane etc. Sistemul trebuie de asemenea să permită stabilirea acelor acte vitale — actele esențiale pentru continuitatea activității după un dezastru natural (incendiu, inundație, cutremur) sau tulburări sociale (revoluție, război etc.), care trebuie să fie disponibile într-un astfel de caz. În fine, un ERMS trebuie să aibă funcționalități robuste pentru dispoziție — proces care acoperă toată gama de acțiuni care permit scoaterea unui act de sub administrarea sistemului (selecționare, distrugere, transfer către alt depozit sau alt ERMS). Deosebirile de bază dintre un sistem de management al documentelor și unul de management al actelor ar fi:

Un sistem de management al documentelor	**Un sistem de management al actelor…**
…permite documentelor să fie modificate	…protejează actele de modificări
…permite documentelor să existe în câteva versiuni	…permite existența unei singure versiuni finale a actului
…poate permite ca responsabilii să își șteargă documentele	…protejează actele împotriva ștergerii, cu excepția unor situații strict controlate
…poate include o evidență de păstrare	…trebuie să includă o evidență riguroasă de păstrare
…poate include o structură de stocare a documentelor, care poate fi sub controlul utilizatorilor	…trebuie să includă o structură riguroasă de ordonare a actelor (schema de clasificare), care este întreținută de rolul de administrator
…este destinat în primul rând să sprijine folosirea zilnică a documentelor pentru activități în desfășurare	…poate sprijini activitatea zilnică, dar este gândit în primul rând să furnizeze un depozit sigur pentru actele rezultate din

[15] Sensul este cel clasic, de repartizare după anumite criterii într-o clasă; nu are semnificația de „secret”.

Un sistem de management al documentelor	Un sistem de management al actelor…
	activitate.

Acest model de bună practică a fost urmat și de alte structuri guvernamentale americane (DoD 5052.2 devenind reper pentru toate software-urile guvernamentale, civile sau militare, deopotrivă), dar și în exteriorul SUA. Dintr-o dată, guvernanții, decidenții și arhiviștii au realizat că există o legislație referitoare fie la arhive, fie la managementul actelor; că este necesar să se facă diferența dintre un simplu e-mail de un mail instituțional, ce trebuie păstrat ca dovadă a activității; că nu toate „documentele" electronice trebuie păstrate pentru totdeauna și trebuie făcută o selecționare; că simpla indexare nu oferă suficient context pentru a înțelege o grupare de acte. Pentru toate acestea este nevoie de funcționalități, dacă nu chiar de un sistem de management a actelor.

Statelor Unite le-a urmat acțiunea guvernului britanic. În 1999, într-un material prezentat de primul ministru, Tony Blair, în fața Parlamentului, referitor la modernizarea guvernării, se menționa că „scopul nostru este ca, până în anul 2004, toate nou-createle acte ale instituțiilor publice să fie stocate și regăsite electronic"[16]. Pentru a îndeplini acest obiectiv, Arhivele Naționale britanice (atunci PRO — Public Records Office) au demarat un program amplu de întocmire și difuzare de linii directoare și proceduri pentru instituțiile publice, astfel încât administrarea actelor electronice să satisfacă cerințele legale și profesionale. Ca urmare, în 1999 și în 2002 au fost emise două seturi de cerințe funcționale ce descriau un sistem de management al actelor electronice pentru administrația publică; în 2002 a fost dezvoltat și un program de testare al aplicațiilor care considerau că îndeplinesc acele cerințe. Ulterior, doar software-urile certificate puteau fi implementate în administrația publică. În anii următori, diverse țări și-au întocmit astfel de cerințe[17]; experiența și pragmatismul excepțional al specificațiilor britanice au rămas însă un model neegalat și o referință pentru toate specificațiile ulterioare, în Europa și în afara acesteia[18].

b). MoReq

A fost evident pentru cei care au încercat să implementeze în Europa DoD 5015.2 că prevederile sale se aplicau greu/erau inaplicabile/erau incomplete pentru administrația europeană. Se impunea așadar, într-o Europă care tindea să devină digitală, creionarea unei poziții proprii, adaptate. În anul 2001, Comisia Europeană a finanțat dezvoltarea și publicarea MoReq — Cerințe model pentru sistemele de administrare a actelor electronice[19] de către Forumul DLM[20]. Cerințele au fost puternic influențate de sistemul britanic, iar judecând după impact (ca număr de traduceri, referințe și reproduceri) a fost un succes deosebit. Cu toate acestea, lipsa unui cadru de testare a conformității, evoluția tehnologică și conceptuală a impus nevoia unei noi specificații. Acesta, după un proces de analiză, consultare și elaborare de 3 ani, a fost publicat în 2008 — MoReq2, a cărui versiune în limba română este cuprinsă în acest volum.

c). MoReq2 în limba română — pentru ce?

Sunt necesare câteva considerații despre MoReq2 și motivele pentru care este relevant pentru cititorul român. În primul rând, este primul și singurul document de acest gen publicat în limba română. Și, până la

[16] *Modernising Government*, 1999 la http://www.archive.official-documents.co.uk/document/cm43/4310/4310-05.htm.
[17] O listă destul de cuprinzătoare la http://moreq2.eu/other-specifications.
[18] Este de remarcat însă și faptul că diferențele de administrație, legislație, cultură informatică etc. au creat tensiuni în adaptarea identică a acestor specificații și au obligat, nu de puține ori, la adaptări naționale. Influența covârșitoare a specificațiilor brtanice rămâne însă de necontestat.
[19] *Model Requirements For Electronic Records Management Systems*, Bruxelles, 2001.
[20] Forumul DLM este o fundație europeană, apropiată Comisiei Europene, destinată reunirii instituțiilor, organizațiilor și persoanelor interesate de managementul documentelor și arhivelor.

publicarea traducerii în limba română a MoReq2010[21], rămâne cel mai bun manual de ERM publicat în limba română. Este de remarcat că dezbaterile profesionale în România sunt rare și, atunci când ele există, sunt axate covârșitor pe arhivistica tradițională. Articolele și intervențiile, izolate, pe tema arhivisticii electronice sunt nearticulate și nu există vreo lucrare de sinteză, integratoare, pentru aceste subiecte. MoReq2 este, pentru partea activă din ciclul de viață a actelor, un document de excepție, care oferă perspectiva integratoare, atât de necesară.

În al doilea rând, așa cum menționam mai sus, este un document care respiră prin toți porii pragmatismul arhivistic. Deși este o specificație pentru un software, conceptele, terminologia și procesele sunt mai degrabă inteligibile pentru arhiviști. Din acest punct de vedere, MoReq2 este cea mai bună introducere pentru un arhivist tradițional în domeniul managementului actelor electronice. În egală măsură, reprezintă cea mai lină trecere de la arhivistica clasică la cea electronică. Sunt fraze memorabile, sunt evaluări mature, sunt explicații care rămân valabile atât pentru managementul actelor electronice, cât și pentru cele tradiționale.

În al treilea rând, prezentul material este util pentru cei care activează, fie ca proiectanți și dezvoltatori software, fie ca beneficiari, în domeniul managementului actelor electronice, incluzând aici și „arhivarea" electronică. Abordarea este validă, principiile și modelul conceptual sunt valabile și aduc o neîndoielnică perfecționare a vizunii curente, obișnuite, asupra administrării entităților electronice.

d). MoReq2 — copilul bătrân

S-a remarcat poate, din cele spuse mai sus, că nu am făcut nici un fel de mențiuni despre folosirea MoReq2 pentru ceea ce a fost destinat: model pentru realizarea caietelor de sarcini în vederea achiziționării unui sistem SMAE (ERMS). Omisiunea este intenționată și este datorată evoluțiilor ulterioare anului 2008.

În momentul în care am început să traducem MoReq2 în limba română, încă din anul 2007, acesta se anunța a fi reperul modernității. Întâlnirile Forumului DLM[22] în care se discutau diferitele capitole așteptau cu încredere produsul, iar intervențiile critice (despre direcțiile diferite de evoluție a tehnologiilor, despre exigențele exagerate ale specificației pentru organizațiile obișnuite și costurile foarte mari pe care le-ar fi implicat dezvoltarea de ERMS conforme) păreau izolate și nesemnificative. Conferința de la Toulouse (2008) a marcat un triumf al MoReq2, traducerile au explodat peste tot în lume (peste 10 traduceri în mai puțin de 2 ani), iar unele state (Cehia, de pildă) au impus MoReq2 ca standard național. Peste doar un an însă, lovitură de teatru: Forumul DLM a decis rescrierea MoReq2, folosind exact argumentele celor ce păreau izolați și nesemnificativi: specificația este prea mare și, prin urmare, greu de citit și de înțeles; costurile de dezvoltare sunt prea mari; tehnologia oferă alternative serioase la cerințele MoReq2. Ceea ce părea o „revizuire" a devenit însă un produs de sine stătător (MoReq2010), cu o abordare diferită, care a „îngropat" nu atât MoReq2, ci însăși lumea pe care MoReq2 o întruchipa: ERMS…

Să detaliem puțin. MoReq2 a fost dezvoltat de oamenii care participaseră și la dezvoltarea cerințelor emise de Arhivele Naționale ale Marii Britanii. Abordarea lor a fost, cum spuneam mai sus, una extrem de pragmatică: așa se întâmplă în lumea fizică, să aplicăm aceleași principii și în spațiul virtual. Și așa au rezultat documente, înregistrări (captură și declarare) de acte, dosare, scheme de clasificare, selecționări, distrugeri etc. Vocabularul din arhivistica clasică a fost transferat spre IT; acolo unde realitatea impunea noi termeni, ei au fost „inventați", plecând însă tot de la realitățile arhivistice. A rezultat o aplicație software care îndeplinea toate aceste cerințe și care a fost definită drept un sistem de management al actelor electronice (e*lectronic records management system* — ERMS). Caracteristica lui de bază era implementarea

[21] Acțiunea de traducere a început, într-un proiect împreună cu studenți ai Facultății de Arhivistică din București.
[22] La care am fost martor direct (Berlin și Lisabona, 2007, Toulouse, 2008).

de controale de siguranță asupra ciclului de viață a unui act, răspunzând astfel exigențelor legale referitoare la păstrarea actelor. Pentru utilizator însă era un efort suplimentar; pentru furnizor, configurarea tuturor controalelor, precum și integrarea cu aplicațiile software de activitate costau enorm[23]. Și, în plus, modul de creare și constituire al documentelor electronice (digitale) a depășit ceea ce se știa anterior din lumea fizică; documentul electronic este, așadar, tot ceea ce era documentul pe hârtie sau o înregistrare audio-video etc., dar și ceva în plus… Tehnologia evoluase, așteptările oamenilor s-au modificat, părea momentul să se schimbe și abordările.

Mai mult, un studiu de impact din 2008 al Arhivelor Naționale britanice (TNA) analiza situația implementării ERMS în administrația Regatului Unit[24]. Bilanțul era devastator:

Abordarea strategică:

- Nu se putea implementa un singur model de sistem pentru toate instituțiile guvernamentale; existau nevoi specifice, dar nimeni nu se ocupa de adaptarea cerințelor generice (emise de Arhivele Naționale) la nevoile specifice.
- Implementarea sistemelor presupunea o strategie și o sincronizare la nivelul instituțiilor — ceea ce adesea lipsea și rezultau în mai multe implementări de produse diferite, care duceau la lipsa de comunicare între structuri ale aceleiași organizații.
- ERMS nu sprijineau, prin modul lor de funcționare, activitatea instituțiilor; deși managementul actelor trebuia să fie o funcție suport, prin implementarea ERMS se ajungea ca acest management să fie o activitate în sine.
- ERMS nu erau folosite pentru administrarea tuturor informațiilor din alte sisteme informaționale, astfel încât accesul la informații era fragmentat.
- ERM nu erau folosite pentru administrarea tuturor tipurilor de informații și nu se făcea diferența între informațiile ce trebuiau păstrate și cele temporare.
- Asigurarea de către guvern a dezvoltării cerințelor și a unui program de testare nu a fost sustenabilă, datorită costurilor și necesarului de personal.

Implementarea ERMS

- În cadrul instituțiilor nu erau folosite doar sisteme aprobate, ceea ce implicit ducea la încălcarea cerințelor oficiale și la administrarea cu dificultate a actelor.
- Implementarea ERMS era extrem de costisitoare
- Ar fi fost necesar un program intensiv de management al schimbării, pentru a pregăti funcționarii în utilizarea sistemelor
- Schemele de clasificare nu erau înțelese de utilizatori
- Nu exista experiență în implementarea sistemelor ERMS, atât la nivelul furnizorilor, cât și la nivelul instituțiilor guvernamentale
- Nu exista sprijin post-implementare

Experiența utilizării ERMS

- Sistemele nu au funcționat întotdeauna în mediul de producție, datorită scalabilității limitate, slăbiciunii aparatelor și rețelei etc.
- Cerințele TNA au generat sisteme prea complexe față de necesități
- ERMS nu erau prietenoase cu utilizatorul

[23] *RMS Debate: The case against EDRMS: Has EDRMS been a success? The case for the prosecution*, la ,,RMS Conference", Edinburgh 22 April 2007, publicat la https://docs.google.com/document/pub?id=1HAvmy87baTm6h0R3_eEgAKz1mK1YwbYviiefUEZSpDs. Cuvintele lui Steve Bailey sunt extreme de dure: ,,As far as the average user is concerned, the EDRMS is something they didn't want, don't like and can't use"; "These EDRM systems [are] systems designed for the convenience and benefit of the records manager at the expense of everyone else". Alte poziții pe aceeași temă: Julie McLeod, *Managing electronic records. Systems/technology approaches for your organization*, prezentare la ,,Managing Electronic Records: Seminars on Technology Approaches and 'Future of RM in a Web 2.0 world", Icelandic Records Management Association, Reykjavik 9 April 2010, publicat la http://www.northumbria.ac.uk/static/5007/ceispdf/final.pdf. Julie McLeod a desfășurat, de altfel, la Universitatea Northumbria, un proiect de cercetare în acest sens (http://www.northumbria.ac.uk/sd/academic/ceis/re/isrc/themes/rmarea/erm/) ale cărui rezultate sunt publicate (http://www.northumbria.ac.uk/static/5007/ceispdf/final.pdf).

[24] Rezultatele acestui studiu ne-au fost aduse la cunoștință informal, cu ocazia unei conferințe.

- Lucrătorii au salvat informațiile în afara sistemului și, deci, în afara controlului ERMS

Cultura managementului informației

- Cultura păstrării actelor în serviciul public era pe cale de dispariție
- Implementarea ERMS producea schimbări în cultura existentă de management a actelor.
- Managementul informațiilor nu a fost sprijinit de conducere.

În aceste condiții, la nivelul anului 2008 se punea în discuție utilitatea însăși a ERMS și se ivea, la nivelul industriei, provocarea găsirii unei alternative. Acea alternativă exista și, grație dezvoltărilor tehnologice, era din ce în ce mai eficientă: soluția integrată a sistemelor de management al conținutului a întreprinderii (ECM). „Dezintegrând" documentul sau actul, aceste sisteme pornesc de la premisa că „orice este conținut" (informație), iar un act sau un document este doar un caz particular (o manifestare sau o reprezentare) a acestuia. Aceste sisteme integrează practic funcționalități care anterior aveau sisteme dedicate, cum ar fi *imaging*, *document* și *records management* etc.[25].

Ca urmare, deși MoReq2 a îndeplinit cerințele solicitate de beneficiari (Forumul DLM și Comisia Europeană), el a reprezentat cea mai complexă descriere a unor sisteme software specializate; dar aceste sisteme erau muribunde. MoReq2 este apogeul unei soluții profesionale — ERMS. Sistemele tip ERMS erau însă (și sunt încă) produse la capăt de drum. MoReq2 era, în 2008, un copil, nou-născut — dar deja bătrân.

În fapt, cerințele anterioare pentru sistemele dedicate managementului actelor trebuiau să devină cerințe pentru funcționalități specifice, ce vor fi îndeplinite de module din aplicații software de activitate specifică (*business systems*) sau din sisteme complexe de management al conținutului. Din acest motiv, Forumul DLM a fost pus într-o postură extrem de dificilă în anul 2009, când a fost obligat de viața reală (întruchipată poate de firmele IT…) să ia în calcul „revizuirea" MoReq2: tot volumul de muncă de creare, difuzare, traducere, implementare a MoReq2 s-a dovedit a fi irosit și inutil. Și nu e de neglijat nici bugetul aferent… Reacțiile comunității de utilizatori a fost pe măsură: o reacție între respingerea modificărilor și un sentiment de trădare și frustrare, generat de inutilitatea muncii depuse în legătură cu MoReq2. La toate acestea, s-a adăugat surpriza MoReq2010: deși s-a spus că e doar o simplificare a MoReq2, noua specificație s-a dovedit a fi cu mult mai complexă: cel puțin dublă ca număr de pagini, cu o abordare orientată spre IT și o interpretare extrem de abstractă și esențializată a principiilor și tehnicilor de management al actelor. Toate acestea au stârnit protestele vehemente ale arhiviștilor obișnuiți cu sistemele „clasice"[26].

Astăzi, nu există încă nici un sistem conform MoReq2010. Există în schimb cel puțin un produs certificat conform MoReq2 și alte două care au anunțat intenția de testare pentru conformitate[27]. Așadar, deși MoReq2010 reprezintă în mod clar viitorul și are o abordare care deschide perspective pline de speranță justificată asupra eficienței și existenței în viitor a managementului actelor electronice, MoReq2, ca reprezentant al Lumii Vechi, încă are un rol de jucat.

Aceste argumente au stat la baza deciziei noastre de finalizare și publicare a orezentei traduceri în limba română.

[25] Vezi o prezentare sintetică la http://en.wikipedia.org/wiki/Enterprise_content_management.
[26] Autorul acestor rânduri a fost membru în Comitetul de revizori al MoReq2010 și martor la cele relatate.
[27] http://www.moreq2.eu/press-a-web/emc/categories/13_0a21e797355278595a6db0d6a0e2936e, http://www.moreq2.eu/press-a-web/fabasoft/categories/12_6cb673dd3ff363f402d07506094516dc, http://www.moreq2.eu/press-a-web/open-text/categories/14_23c43dafae2708f2750807d68f807594.

e). Precizări legate de traducere

În condițiile în care arhivistica românească nu are parte de prea multe traduceri, limba română excelează în polisemantism și, adesea, lipsa de precizie în definirea noțiunilor[28], iar „modernizarea" postdecembristă a introdus „romgleza"[29], de neînțeles pentru vorbitorii normali de limbă română, traducerea MoReq2 a fost o provocare majoră, tehnică și filologică. Pe de o parte, scopul nostru a fost acela de a reproduce în românește semnificația tehnică termenilor și fenomenelor; pe de altă parte, intenția a fost aceea de a pune textul într-o cât mai curată limba română, chiar cu riscul de a nu mai fi inteligibili pentru cei ce folosesc jargonul „romglez" al zilei. Din aceste motive, simțim nevoia unor precizări suplimentare și a unor justificări pentru anumite opțiuni de traducere.

RECORD

Termenul *record* a făcut înconjurul Europei și a constituit poate cel mai dezbătut termen din MoReq la reuniunile DLM. Toți cei implicați în crearea/traducerea/citirea MoReq (indiferent de versiune) știu că acest termen este unul generator de probleme.

Termenul *record* este unul specific limbii engleze. Iată câteva definiții:

Longman:

RECORD = information about something that is written down or stored on computer, film etc., so that it can be looked at in the future[30]

Dicţionar Oxford Explicativ Ilustrat al limbii engleze[31]

RECORD = a). a piece of evidence or information constituting an account of something that has occured, being set etc.; b). a document preserving this; c).the state of being set down or preserved in writing or some other permanent form etc.

Britannica[32], **Merriam Webster**[33]

RECORD= to set down in writing: furnish written evidence of

ISO 15489-1

RECORD = ,,information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business"

Paradoxul face ca, deși *record* nu are un echivalent în limbile romanice, termenul să provină din latină:

- **recordatio**: reamintire, evocare
- **recordo**: a reaminti
- **recordor**: a-și reaminti[34]

Termenul record definește așadar un tip de document (o informație, în accepțiunea actuală), care este păstrat pentru reamintire, în viitor. Cuvântul a fost folosit în literatura de specialitate anglo-saxonă cu mult

[28] Vezi, de pildă, definiții pentru *act* sau *document*, ca exemple de definiții circulare.
[29] Vezi, de pildă, ,,a salva"în limbaj IT, când sensul, și în engleză și în română ar fi acela de ,,a păstra".
[30] *Longman Dictionary of Contemporary English*, ediție online.
[31] *Dicţionarul Oxford explicativ ilustrat al limbii engleze*, Oxford University Press, Litera Internațional, 2005, sub voce.
[32] www.britannica.com.
[33] www.merriam-webster.com.
[34] Gh. Guțu, *Dicționar latin-român*, București, Edit. Academiei, sub voce.

timp înainte ca sistemele informatice să apară și s-a preluat automat în industria IT, tocmai pentru că făcea diferența între o informație volatilă și una care se păstra[35].

Literatura arhivistică a limbilor romanice are însă o altă abordare. Din motive neclare (și care oricum nu fac obiectul prezentării de față), în franceză, spaniolă, italiană etc. unicul termen desemnat pentru a acoperi definiția englezească este cel de „document". Abordarea arhivistică globală este de altfel diferită, în tradiție romanică existând „arhive" (de la crearea documentului și până la sfârșitul vieții acestuia) spre deosebire de limba engleză, unde există „records" (arhivele „active"și „semiactive") și „archives" (arhive istorice).

Este așadar vorba despre o diferență culturală, în primul rând. Problema a fost ignorată mult timp în sistemele arhivistice tradiționale. În momentul în care standardele internaționale au început să se răspândească pe baza experienței anglo-saxone (vezi, de pildă, standardele ISO 9001 sau 15489), când industria IT, inițial în țări vorbitoare de limbă engleză, a început să facă diferența între sisteme *Document Management* și sisteme *Records Management*, era evident că și „ceilalți" trebuiau să găsească niște echivalențe, mai precise decât termenul integrator de „document".

Mergând spre esența lucrurilor, „document" este termenul generic, reprezentând orice informație consemnată (adică nevolatilă). „Record" este acel document care are o serie de caracteristici suplimentare (se referă la organizație sau persoană, este necesar pentru organizație sau persoană, are o valoare de mărturie/probă). Dacă în sistemele tradiționale era relativ simplu de diferențiat între cei doi termeni (o ciornă era ușor de diferențiat de versiunea finală, la o simplă privire), în sistemul digital acest lucru nu mai este posibil. Exemplul clasic pentru a arăta diferența este cel al unui e-mail: între un mesaj de invitație la masă și un mesaj de convocare pentru ședință a aceleiași persoane nu este, din punct de vedere al formei, nici o diferență: care dintre ele trebuie păstrate? Desigur, cel care este declarat *record*, și este înregistrat ca atare în evidență.

Practica arhivistică românească are un avantaj, în acest sens, față de cea franceză (și revenim imediat cu justificarea comparației cu spațiul francez). România a păstrat sistemul de registratură, astfel încât, prin analogie, putem delimita momentul în care documentul–*document* devine document–*record*. Mai mult, cineva care are cunoștință de istoria arhivisticii românești poate identifica și un nume pentru acest document–*record*, nume care apare în normele de registratură emise în perioada interbelică: „o hârtie înregistrată, indiferent de conținutul ei, se numește *act*"[36]. Acest raționament a stat la baza deciziei noastre de a traduce termenul de *record* ca ***act*.**

Desigur, actul este, în dicționare și în uzul comun al limbii române actuale, legat indisolubil de hârtie. Așa a fost însă și *record* pentru vorbitorii de engleză. Este ilar astăzi să spui că o pagină web poate fi *act*; așa a fost și la ei. Această diferență de întrebuințare este însă cea mai clară expresie a diferenței conceptuale și metodice dintre practica arhivistică românească și cea de limbă engleză; revine tehnicienilor să impună noile semnificații și în limba română.

Am făcut mai sus o comparație cu practica franceză; alegerea Franței în comparația respectivă nu este întâmplătoare. Franța, în încercarea de adoptare a multor standarde scrise inițial în engleză, s-a lovit prima, dintre limbile romanice, de problema traducerii unor termeni. Desigur, acest proces a fost cumva complicat și de mania refuzului anglicismelor în limbă și inventarea unor cuvinte proprii. Din păcate, în cazul concret al termenului *record*, opțiunea inițială a AFNOR (Asociația franceză de standardizare) a fost dezastruoasă și

[35] Vezi folosirea cuvântului în cele două context (înainte și după dezvoltarea actelor electronice) în Mary F. Robek, Gerald F. Brown, David O. Stephens, *Information and Records Management: Document-Based Information Systems*, David O. Stephens, ed. 4, 1995. Vezi, de asemenea, definiția din Wikipedia: ,, A record can be either a tangible object or digital information: for example, birth certificates, medical x-rays, office documents, databases, application data and e-mail".

[36] *Instrucțiuni generale pentru raționalizara și simplificarea lucrărilor de birou*, București, 1942, p. 20.

a cauzat mari probleme, atât pentru profesioniștii francezi din domeniul arhivistic, cât și pentru (în cazul nostru) terminologia de limbă română. Opțiunea inițială a AFNOR a fost traducerea termenului *record* ca „înregistrare" (*enregistrement*). În primul rând, astfel de traducere este greșită filologic. În engleză, „înregistrare" (video, audio etc.) este „recording". Verbul (*to record*) poate însemna „a înregistra", dar în primul rând „a consemna", „a înscrie". Oricare variantă s-ar accepta, *record* nu este „înregistrare", văzut ca document. Traducerea nefericită a stârnit preocuparea arhiviștilor francezi; în ultimele variante de traducere, ei s-au oprit la forma „document d'archives"[37] sau „document d'activité"[38] pentru a reproduce semnificația termenului *record*, dar, sub nici o formă nu au acceptat termenul „înregistrare".

Din păcate, traducerile în limba română au copiat traducerea franceză. Astfel, în versiunea românească a ISO 9001, se vorbește despre „documente" și „înregistrări" (*documents* și *records*) ale proceselor de calitate; în nefericita traducere SR ISO 15489 se vorbește din nou despre dosare cu „înregistrări". Este o expresie a traducerilor făcute de persoane străine domeniului profesional în care traduc și care nu înțeleg semnificația termenului, făcând o echivalare strict lingvistică (și, uneori, nici atât, după cum am văzut). În opinia noastră, este absolut necesară corectarea acestor erori tehnice sau, măcar, corectarea lor în materialele străine, de unde apoi să copieze și traducătorii noștri…

ELECTRONIC RECORDS MANAGEMENT SYSTEM

O altă opțiune, legată de termenul *record* și care, de această dată, vine în contradicție cu o definiție legală din România[39] este cea a traducerii ERMS. *Legea arhivării electronice* definește „sistemul electronic de arhivare — sistemul informatic destinat colectării, stocării, organizării și catalogării documentelor în formă electronică în scopul conservării, consultării și redării acestora". Similaritatea cu franțuzescul „systeme d'archivage electronique" (SAE) este evidentă! Problema este și aici de natură conceptuală. Practica documentelor/actelor pe hârtie din România a exclus (discutabil) termenul „arhivare", considerat imprecis și neprofesional. O definiție comună a arhivării este „operațiunea prin care documentele clasate, constituite în «dosare» după norme prestabilite, se depun și se păstrează în depozite special amenajate și organizate, denumite arhive"[40]. Din punct de vedere tehnic, s-a considerat așadar că „arhivarea" acoperă ,,constituirea dosarelor", respectiv „predarea către depozitul de arhivă" (expresii folosite în legislația actuală). După cum se poate remarca, definiția *arhivării* nu are nici o legătură cu colectarea, stocarea și catalogarea, nici cu scopul realizării unei activități. În franceză, pe de altă parte, SAE este considerat sinonim cu ERMS, însă s-a subliniat și acolo faptul că folosirea termenului„archivage" este greșită, iar sistemele ar trebui să fie denumite „sisteme pentru ciclul de viață a documentelor"[41]. Prin urmare, folosirea denumirii de *sistem de arhivare electronică* este eronată în limba română, iar formularea din lege ar trebui revizuită. Pe de altă parte, remarcăm că arhivistica românească nu are un termen care să definească colectiv partea arhivisticii care se ocupă de arhivele la creatori (înainte de preluarea la arhivele istorice). În această situație, am considerat că traducerea directă „managementul actelor" poate fi o denumire acceptabilă, cel puțin pentru moment și sintagma de „**sistem de management a actelor electronice**" (respectiv „**sistem de management a documentelor electronice**" pentru EDMS) a fost folosită constant în această traducere.

MANAGEMENT

O altă problemă în cursul traducerii a fost opțiunea pentru termenii management – administrare – gestiune. Dacă management este un cuvânt impus relativ nou în limbă, administrare și gestiune există de

[37] G. Drouhet, G. Keslassy, E. Morineau, *Records management: mode d' emploi*, Paris, 2000, p. 9.
[38] Vezi FR ISO 30300.
[39] Definiția sistemului electronic de arhivare din Legea nr. 135/2007: Legea privind arhivarea documentelor în formă electronică.
[40] A. Hascal, L. Popescu, *Corespondență și tehnica secretariatului*, București, 1996, p. 49.
[41] ,,Dans le SAE, le mot «archivage» doit être remplacé par «de cycle de vie du document» et non dans le sens simpliste de «stockage de fichiers»" (http://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27archivage_%C3%A9lectronique).

mult, dar limitele și relațiile dintre ele sunt neclare. *Gestiunea* este definită ca administrare; *administrarea* este definită ca și conducere, organizare; *managementul* este definit ca ansamblu de conducere, organizare, gestiune. Din aceste definiții, rezultă că managementul înglobează administrarea și gestiunea, iar gestiunea este o formă de administrare. Mai mult, managementul, ca și concept, are o întreagă filozofie în spate, fiind definite foarte clar funcțiile specifice (planificare, organizare, conducere, monitorizare, evaluare). Având în vedere toate aceste aspecte, am decis să întrebuințăm termenul „**management**" și în limba română, pentru cuvântul omonim englezesc; acolo unde exista verbul (*to manage*), am optat pentru folosirea termenului „**a administra**".

ATTACHMENT

Așa cum e-mail-ul este „scrisoarea electronică", la fel ceea ce este pus lângă scrisoare este o „**anexă**". Reamintim că „atașamentul" are o cu totul altă semnificație decât un document anexat.

DIGITIZE

Un alt termen care a impus o decizie este echivalentul românesc al lui „to digitize". Remarcăm că, exceptând limba franceză (care are forma *numerisation*), toate celelalte limbi romanice folosesc termenul *digitalizare*: *digitalizzare* (italiană), *digitalizar* (portugheză și spaniolă); la fel și alte limbi europene (*digitalisieren* (germană), *digitalizálni* (maghiară), *digitalizacji* (poloneză) etc.). În plus, forma *digitalizare* există în limba română de cel puțin 30 de ani, fiind de altfel singura formă acceptată oficial de DEX. Cu toate acestea, mai ales în zona bibliotecilor, se întrebuințează (mai mult prin contagiune decât asumat conștient) termenul „digitizare" — calc evident după limba engleză, care dublează termenul deja existent în românește. În traducerea acestui material, am considerat corect să nu dăm curs formelor inițiate, probabil, de cineva insuficient de pus la punct cu echivalentele românești ale limbii engleze și, ca urmare, am folosit termenul „**digitalizare**".

DISPOSITION

Deși verbul „to dispose" semnifică eliminarea, termenul *disposition* (sau *disposal*) în contextul managementului actelor are o semnificație mai nuanțată. Conform ISO 1548-1, *disposition* înseamnă una din următoarele acțiuni:

a). o distrugere imediată, incluzând suprascrierea sau ştergerea

b). reţinerea, pentru o perioadă ulterioară, în cadrul diviziunii administrative

c). transferul către o zonă de depozitare corespunzătoare sau pe un suport, sub controlul organizaţiei

d). transferul către altă organizaţie care are asumată responsabilitatea pentru afacerea respectivă, prin restructurare, vânzare sau privatizare

e). transferul către o zonă de depozitare gestionată în numele organizaţiei de către un furnizor independent, faţă de care au fost stabilite aranjamente contractuale corespunzătoare

f). transferul de responsabilitate pentru gestionare către o autoritate corespunzătoare, în timp ce depozitarea fizică a documentului este reţinută de organizaţia creatoare

g). transferul către arhiva organizaţiei

h). transferul către o autoritate de arhive istorice externă.

Așadar, *disposition* reflectă o decizia asupra destinului viitor al unor acte/documente. Termenul omolog din limba română („dispoziție") are un sens specific în dreptul civil[42], care acoperă în bună măsură sensul englezesc din context. Din acest motiv, am optat pentru folosirea termenului „**dispoziție**", ca reflectare a unui termen tehnic din arhivistica anglo-saxonă.

DISTRIBUTED

Deși jargonul IT a consacrat calchierea „distribuit", este simplu de constatat că acest termen românesc nu reproduce sensul englezesc. De aceea, am preferat folosirea termenului „**dispersat**", care reflectă semnificația englezească și în limba română.

OWNER

În ciuda aparentei simplități a traducerii, *owner* nu înseamnă, în contextul MoReq2, *proprietar*. *Owner* este persoana care deține responsabilitatea de creare a actului. Cum în limba engleză *responsible* are doar funcție de adjectiv, termenul *owner* acoperă și semnificația substantivului „***responsabil"*** din limba română.

TYPE (OF RECORDS)

În lumea IT se vorbește tot mai frecvent despre *tipuri de acte (documente)*. Analizând definiția tehnică a termenului în limba engleză[43], se poate constata că *record type* este echivalentul ,,**genului documentului**" din arhivistica românească.

FILE/FOLDER

Ambii termeni pot fi traduși prin cuvântul „**dosar**". Diferența rezidă în faptul că *file* se referă la conținutul intelectual al grupării de acte (ca în expresia ,,dosar personal"), în timp ce *folder* se referă la copertele în care se adună respectiva grupare („dosar cu șină")

PARENT/CHILD

Deși frecvent descrise în limba română sub forma *subordonat/supraordonat*, raporturile definite astfel nu exprimă în mod precis relațiile pe care le descriu termenii englezești. Este opoziția clasificărilor arborescente („bicicletă > cadru, roți, ghidon"), față de clasificările ierarhice („regn animal > mamifer > om"). În clasificările ierarhice, elementul subordonat „moștenește" anumite caracteristici de la elementul supraordonat, așa cum copilul moștenește de la părinte; această nuanță nu este transmisă de formularea subordonat/supraordonat. Ca urmare, am considerat necesară folosirea terminologiei traduse din engleză, raporturi „**părinte/copil"**.

RETENTION AND DISPOZITION SCHEDULE

Legat de dispoziție apare și un instrument specific arhivisticii anglo-saxone, *retention and disposition schedule* (RDS). Tehnic, instrumentul are aceeași funcție ca fostul indicator al termenelor de păstrare din arhivistica românească, dar conținutul RDS este ușor diferit: pe lângă termenele de păstrare, RDS cuprinde și acțiunile de dispoziție care vor fi efectuate asupra unei categorii de acte, la momentul scadent. Am folosit traducerea „**programare de păstrare și dispoziție**".

---

[42] ,,*Dreptul de dispoziție* este alcătuit din dreptul de dispoziție materială și dreptul de dispoziție juridică. *Dreptul de dispoziție materială* este posibilitatea proprietarului de a dispune de substanța bunului, adică de a-l transforma, consuma sau distruge, cu respectarea reglementărilor în vigoare. *Dreptul de dispoziție juridică* se concretizează în posibilitatea proprietarului de a înstrăina dreptul de proprietate, cu titlu oneros sau gratuit, prin acte între vii sau *mortis causa* și de a-l greva cu drepturi reale derivate, principale sau accesorii, în favoarea altor persoane, cu respectarea regimului juridic stabilit de lege" (http://www.rubinian.com/dictionar_detalii.php?id=478).

[43] http://www.archivists.org/glossary/term_details.asp?DefinitionKey=1033.

RETENTION, PRESERVATION

În limba român, termenul ,,a păstra” poate avea mai multe semnificații, fiecare desemnată cu alt cuvânt în engleză:

a păstra	a nu elimina	*retention*
	a nu deteriora	*preservation*
	a ține	*keeping*
	a menține	*maintain*

SECURITY CATEGORY

Deși terminologia ce definește documentele clasificate (secrete) din România este aliniată la cea de limbă engleză, autorii MoReq2 au preferat întrebuințarea unor termeni diferiți. Ca urmare, am considerat necesar să subliniem diferențele, dar să folosim terminologia intenționată de autori.

MoReq2	Legislație românească	Exemple
clasă de securitate	nivel de secretizare	secret, strict secret sau strict secret de importanță deosebit
categorie de securitate	clase de secretizare	Secret de serviciu, secret de stat (în cazul MoReq2, și secret comercial, bancar etc.)

CERINȚE MODEL
PENTRU MANAGEMENTUL ACTELOR ELECTRONICE
ACTUALIZARE ŞI DEZVOLTARE, 2008

Specificația MoReq2

Această specificație a fost pregătită de Serco Consulting pentru Comisia Europeană, cu finanțare din partea programului IDABC

CERINȚE MODEL
PENTRU MANAGEMENTUL ACTELOR ELECTRONICE

Actualizare şi dezvoltare, 2008

Specificația MoReq2

Această Specificație este disponibilă în format electronic la următoarele url:

http://dlm-network.org/MoReq2

http://ec.europa.eu/transparency/archival_policy

şi pe alte site-uri. Traducerile în alte limbi sunt aşteptate să fie disponibile la aceste site-uri.

Este de asemenea disponibilă în format fizic (pe hârtie) la Biroul pentru publicații oficiale ale Comunităților Europene ca supliment VIII al INSAR.

Cuprins

Prefață: MoReq2

Actualizarea şi extinderea

Cerințelor Model pentru Managementul Actelor Electronice

De la publicarea sa în 2001, versiunea originală MoReq — Cerinţe Model pentru Managementul Actelor Electronice — a fost larg utilizată în cadrul Europei şi în afara ei. În cadrul Uniunii Europene, utilizatorii potenţiali din zona managementului actelor electronice au recunoscut valoarea utilizării unei specificaţii model, aşa cum este MoReq, ca bază pentru licitaţii în vederea obţinerii de Sisteme de Management al Actelor Electronice, iar furnizorii de aplicaţii informatice au răspuns prin folosirea MoReq pentru a coordona procesul lor de dezvolt are.

MoReq este acum privit ca un succes indiscutabil. A fost citat de multe ori pe multe continente şi are un rol central pe scena managementului actelor electronice.

Cu toate acestea, tehnologia informaţiei s-a modificat din 2001. S-a înregistrat o creştere şi o schimbare evolutivă în multe zone ale tehnologiei, care au afectat crearea, captura şi managementul actelor electronice. Această nouă versiune a MoReq, numită MoReq2, tratează impactul acestei schimbări tehnologice. Ia de asemenea în calcul noile standarde şi bune practici care au fost dezvoltate în ultimii câţiva ani. În consecinţă, MoReq2 a fost scris ca o actualizare evolutivă a MoReq original.

MoReq2 permite de asemenea, pentru prima dată, implementarea unui regim de testare al aplicaţiilor. A fost scris pentru executarea unei testări de conformitate independente şi o serie de astfel de teste au fost elaborate şi publicate în paralel cu cerinţele model. Nevoia unor cerinţe testabile, riguros exprimate, a condus la mai multe schimbări de vocabular şi de exprimare în MoReq2.

În final, anii de experienţă în folosirea şi aplicarea MoReq au relevat nevoia particularismelor naţionale, de a lua în calcul diferitele limbi, legislaţii, reglementări şi tradiţii arhivistice naţionale. Din acest motiv, MoReq2 introduce pentru prima dată un mecanism de moderare — intitulat „Capitolul zero” — pentru a permite statelor membre să adauge cerinţele lor naţionale specifice.

MoReq2 a fost pregătit pentru Comisia Europeană de către firma Serco Consulting, prin finanţarea asigurată de programul IDABC al Uniunii Europene. Procesul de elaborare a fost supervizat de Comisia Europeană, în strânsă cooperare cu Forumul DLM, iar versiunile preliminare au fost revizuite de experţii Forumului DLM, în puncte cheie ale stadiului de dezvoltare. Aceste revizuiri au fost completate cu sugestiile şi revizuirile a zeci de utilizatori, consultanţi, furnizori, structuri academice şi profesionale din întreaga lume, furnizând astfel pentru MoReq2 un nivel de

autoritate fără precedent. Ca urmare, MoReq2 va fi deosebit de valoros pentru toţi cei implicaţi în managementul actelor electronice din Europa şi din lume.

1. Introducere

1.1. Istoric

Nevoia unei specificaţii cuprinzătoare a cerinţelor pentru managementul actelor electronice a fost pentru prima dată formulată de Forumul DLM[1] în 1996 ca unul din cele 10 puncte de acţiune ale sale. Mai departe, programul IDA (*Interchange of Data between Administrations*) al Comisiei Europene a încredinţat dezvoltarea unui model de specificaţie pentru sistemele de management al actelor electronice (SMAE). Rezultatul — MoReq, Cerinţe model pentru managementul actelor electronice[2], a fost publicat în 2001.

MoReq a fost larg folosit în cadrul Uniunii Europeană şi în afara ei. Cu toate acestea, nu a existat nici un regim de mentenanţă pentru MoReq şi nici o schemă de testare a conformităţii softurilor cu specificaţiile MoReq.

Solicitările, atât pentru actualizarea MoReq, cât şi pentru o schemă de testare de conformitate au crescut. Forumul DLM a discutat cu Comisia Europeană. Aceste discuţii au culminat în lansarea de către Secretariatul general al Comisiei (Directoratul B — e-Domec şi arhive) a unei competiţii deschise pentru dezvoltarea acestui document, MoReq2, în 2006. Dezvoltarea a fost realizata în 2007 de către o mică echipă de consultanţi specialişti din cadrul Serco Consulting (anterior Cornwell Management Consultants plc.), sprijinită de un Consiliu editorial de experţi, aleşi din câteva ţări, şi numeroşi recenzori voluntari, atât din sector public, cât şi privat.

Anexa 2 conţine mai multe detalii despre metodologia folosită şi anexa 4 evidenţiază contribuţia membrilor grupului de revizuire care şi-au dedicat voluntar şi cu amabilitate timpul, cunoştinţele şi experienţa lor.

1.2. Relaţia între MoReq şi MoReq2

MoReq2 este destinat să înlocuiască MoReq.

Specificaţiile pentru MoReq2 sunt conţinute în „Raport asupra ariei de aplicare a MoReq2”[3]. Acesta descrie scopurile pentru MoReq2 după cum urmează:

---

[1]DLM este acronimul pentru „Document Lifecycle Management” (anterior a fost acronim pentru expresia franceză: „Données Lisibles par Machine”, în engleză „machine-readable data”. Forumul DLM se bazează pe concluziile Consiliului Europei (94/C 235/03) din 17 iunie 1994, referitoare la intensificarea cooperării în domeniul arhivelor.

[2]MoReq2 este disponibil pe http://www.DLM-Network.org; a fost de asemenea publicat în format pe hârtie cu ISBN 92-894-1290-9.

[3] “Raportul asupra aplicabilităţii MoReq2" este disponibil la http://www.DLM-Network.org.

„Ţintele finale ale dezvoltării MoReq2 sunt să dezvolte cerinţe funcţionale extinse în context european şi să sprijine o schemă de conformitate prin:

- întărirea părţilor din MoReq2care au devenit între timp arii esenţiale şi acoperirea cu claritate a unor noi arii importante de cerinţe.
- asigurarea că cerinţele funcţionale sunt testabile şi dezvoltarea de materiale de testare pentru a permite produselor să fie testate pentru conformitate cu cerinţele.
- realizarea unui sistem modular de cerinţe care să însoţească aplicarea în diferitele medii în care acestea vor fi folosite."

„Pentru a furniza compatibilitate, MoReq2 trebuie să reprezinte o actualizare evolutivă a MoReq original şi nu un produs radical diferit".

Conceptul de „actualizare evolutivă" este fundamental. MoReq2 este aproape în întregime compatibil cu MoReq (micile incompatibilităţi sunt indicate cu precizie); este bazat pe aceleaşi concepte şi, ca document, foloseşte o structură similară.

1.3. Scopul şi adresabilitatea acestei Specificaţii

Această Specificaţie este versiunea a doua a *Cerinţelor model pentru managementul actelor electronice* (MoReq). El se concentrează în principal asupra cerinţelor funcţionale pentru managementul actelor electronice prin intermediul unui Sistem de Management al Actelor Electronice (SMAE)

Această Specificaţie a fost realizată pentru a fi în egală măsură aplicabilă atât pentru organizaţiile din sectorul public, cât şi pentru cele private, care urmăresc să introducă un SMAE sau care doresc să evalueze capacităţile SMAE pe care îl folosesc în prezent.

Deşi Specificaţia se concentrează pe cerinţe funcţionale, se admite că atributele non-funcţionale sunt importante pentru succesul unui SMAE, ca şi pentru oricare alt sistem informaţional. Cu toate acestea, aceste atribute non-funcţionale variază enorm între diferitele medii. În consecinţă, ele sunt identificate, dar sunt descrise doar în linii generale.

Se face de asemenea referire şi la alte cerinţe strâns legate, cum ar fi managementul documentelor sau managementul electronic al actelor fizice (de ex. dosare pe hârtie sau microfilme), dar nu foarte detaliat. Probleme înrudite, cum ar fi digitalizarea şi alte mijloace de creare a actelor electronice, nu se situează în cadrul ariei de aplicare a acestei Specificaţii. La fel, aceasta nu încearcă să acopere problemele practice ale implementării SMAE.

Această Specificaţie a fost redactată plecându-se de la premisa că printre utilizatorii unui SMAE se numără nu doar administratori, manageri de acte sau arhivişti, ci şi personalul obişnuit şi operaţional al organizaţiilor, care folosesc SMAE ca parte a activităţii lor obişnuite, prin crearea, primirea şi regăsirea actelor. Cum această Specificaţie conţine cerinţe „model", ea este proiectată să fie în întregime generică. Nu sunt luate în considerare nici o anumită platformă şi nici un anumit sector. Pentru că este modular, comunităţile de utilizatori îi pot adăuga funcţionalităţi specifice pentru cerinţele activităţii proprii (vezi secţiunea 1.6. şi anexa 3 pentru indicaţii asupra utilizării şi personalizării acestei Specificaţii).

1.4. Ce este un SMAE

Un SMAE este în primul rând o aplicaţie pentru managementul actelor electronice, deşi el poate fi folosit şi pentru managementul actelor fizice. Accentul acestei Specificaţii este pus ferm pe managementul actelor electronice.

Managementul actelor electronice este complex într-o implementare corespunzătoare, solicitând o gamă largă de funcţionalităţi, care să satisfacă nevoile de activitate. În mod obişnuit, un sistem care satisface aceste nevoi — un SMAE — are nevoie de soft specializat, cu toate că funcţionalităţi sporite de management al actelor sunt incluse în softurile tip sistem de operare sau alte aplicaţii. Softurile specializate pot consta fie dintr-un singur pachet, dintr-un număr de pachete integrate, softuri dedicate sau o combinaţie a acestora; şi în toate cazurile este nevoie de manuale de proceduri şi politici de management suplimentare. Natura unui SMAE va varia de la organizaţie la alta. Specificaţia nu face nici un fel de presupuneri asupra naturii soluţiilor SMAE particulare. Utilizatorii Specificaţiei vor trebui să determine modul în care funcţionalitatea unui SMAE poate fi implementată, astfel încât să le satisfacă cerinţele.

Se preconizează ca SMAE să fie folosite pentru perioade de timp îndelungate şi să interacţioneze tot mai mult cu alte aplicații. Există prin urmare mai multe feluri în care un implementator poate dori să conecteze un SMAE cu alte aplicații software. Poate fi necesar să se creeze interfețe pentru captura anumitor acte din alte aplicații implicate în activitate (vezi secțiunea 6.1) şi pentru ca aplicațiile să acceseze acte din SMAE (vezi secțiunea 4.1). Toate acestea se produc în special în cazul aplicațiilor tip *business*, cum ar fi CRM (Managementul relațiilor cu clienții) şi o serie de alte aplicații tip *business*.

Capitolul 10 include elemente specifice de relaționare cu CMS (Sisteme de management al conținutului), sisteme de fluxuri de lucru şi de activități de caz şi integrare fax. Capitolul 6 tratează aspecte legate de interfețele cu aplicații de e-mail în secțiunea 6.3 (managementul e-mail-urilor) şi scanarea şi producerea de imagini digitale în secțiunea6.5. Interfața pentru validarea metadatelor este acoperită în secțiunea 6.1. (captura) şi generarea de rapoarte în 8.3 (imprimarea).

MoReq2 a fost scris în primul rând pentru a descrie aplicaţiile software care sunt proiectate specific pentru a administra acte. Cu toate acestea, mai poate fi utilizat şi pentru formularea rezultatelor urmărite de programul de management al actelor electronice. Astfel, declaraţiile din MoReq2 care afirmă: „Un SMAE trebuie sau ar trebui…” poate fi de asemenea citită ca o formă prescurtată pentru „Sistemul organizaţiei utilizatoare şi/sau platforma furnizorului trebuie sau ar trebui…”. Cititorii MoReq2 trebuie să decidă care cerinţe sunt necesare pentru mediul lor.

Setul complet al cerinţelor MoReq2 poate fi potrivit pentru sisteme de aplicaţii integrate. Totuşi, un subset poate fi mai potrivit în situaţia, de pildă, în care caracteristicile de management al actelor sunt necesare ca parte a managementului de caz sau domeniului de aplicaţii business.

Modulele opţionale *10.5. Fluxuri de lucru*şi *10.6. Managementul de caz* se aplică în special domeniului de aplicaţii business. Totuşi, multe din funcţionalităţile descrise în cerinţele din MoReq2 pot fi de asemenea aplicabile şi trebuie să fie luate în considerare la implementarea acestor sisteme de afaceri.

1.5. Pentru ce poate fi folosită această Specificaţie?

Specificaţia MoReq2 se doreşte a fi folosită:

- **de utilizatorii potenţiali ai unui SMAE**: ca bază pentru pregătirea caietelor de sarcini
- **de către utilizatorii SMAE** : ca bază pentru auditarea sau verificarea SMAE existente
- **de către organizaţiile formatoare**: ca document de referinţă pentru pregătirea în domeniul managementului actelor şi ca material de curs.
- **de către instituţii academice**: ca resursă de predare
- **de către furnizori şi dezvoltatori de SMAE**: să ghideze dezvoltarea produsului prin evidențierea funcţionalităţilor solicitate
- **de către furnizorii de servicii de management al actelor**: să ghideze natura serviciilor pe care le oferă
- **de către potenţiali utilizatori ai serviciilor externalizate de management al actelor**: ca un ajutor în specificarea serviciilor ce urmează a fi procurate.

În plus, atunci când este folosit în documentaţia pentru testare dezvoltată în paralel cu MoReq2, se doreşte a fi folosit:

- **de către furnizori şi dezvoltatori de SMAE**: pentru a testa soluţiile SMAE pentru conformitate cu MoReq2
- **de către utilizatorii SMAE** : pentru a testa implementarea SMAE pentru conformitatea cu MoReq2.

Această Specificație este redactată având în minte caracterul utilizabil. Pe tot parcursul, intenţia a fost să fie dezvoltată o specificație care să fie utilă în practică.

1.6. Drepturi de proprietate intelectuală

Toate drepturile de proprietate intelectuală asupra MoReq2, incluzând numele MoReq2, aparţin Comisiei Europene. Ca urmare, trebuie obținut acordul înaintea oricărei traduceri a MoReq2 sau înainte de publicarea Capitolului 0 — vezi nota oficială pe pagina de titlu. Cererile pentru permisiune trebuie adresate pe pagina Forumului DLM la http://www.dlm-network.org

1.7. Accente şi limitări ale Specificării

Specificaţia MoReq2 este în mod explicit proiectată cu gândul la caracterul ei practic şi utilizabil. Este în primul rând destinată să fie un instrument practic pentru ca organizaţiile să îşi satisfacă nevoile activităţii de management al actelor, atât cele create în format digital, cât şi a celor pe hârtie. Deşi în dezvoltarea ei s-au luat în calcul disciplinele tradiţionale arhivistica şi managementul actelor (*records management*), acestea au fost interpretate într-o manieră corespunzătoare mediului electronic. Astfel, MoReq2a fost dezvoltat luând în calcul atât nevoile administratorilor de acte tradiţionale, cât ai celor de acte electronice.

Cerinţele din MoReq2 ar trebui, dacă vor fi implementate, să rezulte într-un sistem care va administra actele electronice laun nivel dorit de încredere şi integritate, prin combinarea atât a avantajelor modalităţilor electronice de activitate, cât şi a teoriei clasice a managementului actelor. Exemple ale acestei abordări pragmatice includ încorporarea cerinţelor pentru managementul documentelor, fluxul activităţilor, metadate şi alte tehnologii înrudite.

Deşi MoReq2 acoperă o serie largă de categorii de acte, este important de reținut că soluțiile SMAE se referă în principal la acele acte care sunt adesea identificate drept acte „nestructurate”[4]. În termeni simpli, actele nestructurate sunt acelea care conțin informații care se prezintă într-o formă destinată să fie în primul rând utilizate de către persoane. Exemple de acte nestructurate sunt scrisori, referate, mesaje e-mail, imagini, fotocopii, imagini scanate, înregistrări audio şi video. Spre deosebire de acestea, actele structurate conțin informații sub o formă destinată să fie în primul rând folosită de aplicațiile informatice (exemplele includ înregistrările din sistemele de contabilitate electronică, de programare a producției şi ale sistemelor de control al traficului). Deşi un SMAE poate, în principiu, să fie folosit pentru a stoca asemenea acte structurate, rareori se întâmplă acest lucru. În majoritatea situațiilor, datele structurate sunt stocate sub administrarea unei aplicații de prelucrare a datelor (în exemplele de mai sus, acestea ar putea fi contabilitate generală (*general ledger system*)şi sisteme de control al traficului aerian). Soluțiile SMAE sunt aproape universal folosite pentru a stoca şi administra acte nestructurate. Cazurile în care un SMAE este folosit pentru acte structurate se ivesc adesea în mediile de management al cazurilor — vezi secțiunea 10.5.

MoReq2 nu tratează aspectele practice ale managementului actelor. În mod intenționat, Specificația se referă doar la capacitățile cerute pentru managementul actelor electronice de către aplicațiile informatice. Specificația evită discuția despre filozofia managementului actelor, teorie arhivistică, luarea deciziilor, controlul managementului etc.; aceste aspecte sunt bine tratate în alte lucrări, unele dintre ele fiind prezentate în anexa 1. Ca un exemplu specific, Specificația precizează în câteva locuri că anumite funcții trebuie să fie limitate la rolurile de administrator. Această nu înseamnă că rolurile de administrator trebuie să ia decizii de politică organizaţională, ci doar că trebuie să fie singurii utilizatori împuterniciți de organizație să le execute prin intermediul unui SMAE.

Este important de reținut că politica de management al actelor trebuie să fie integrată cu cerințele tehnice şi de activitate ale organizației, şi că un rol de administrator poate doar implementa, din perspectiva managementului actelor şi a sistemului, deciziile luate de managementul de nivel superior.

În fine, această Specificație este în mod intenționat centrată pe utilizator; întrebuințează, pe cât posibil, categoria de terminologie utilizată în mod obişnuit de aceia care operează cu actele electronice. De pildă, Specificația descrie că dosarele electronice „conțin” acte, pentru facilitarea înțelegerii, chiar dacă dosarele electronice nu conțin, strict vorbind, nimic. Vezi secțiunea 2.2 pentru mai multe detalii.

1.8 Considerații pentru fiecare Stat Membru

Aşa cum s-a explicat în secţiunea referitoare la adresabilitate (secţiunea 1.3), această Specificaţie încearcă să acopere o gamă largă de cerinţe, din diferite ţări, din diferite industrii şi cu diferite categorii de acte. Adresabilitatea largă a fost intenţionată; dar ea conduce la o limitare semnificativă, anume că această Specificare nu poate reprezenta singură o cerinţă care să se aşeze

[4] Se poate susține că toate actele electronice administrate corespunzător sunt structurate, de vreme ce ele sunt asociate cu metadatele, cu datele din evidența de auditare etc. într-o manieră structurată. Din această perspectivă, ar fi mai precis ca semnificația termenului actele nestructurate să fie „acte având un conținut nestructurat”; însă această semnificația nu este una obişnuită şi ca urmare nu a fost adoptată de MoReq2.

cu exactitate pe cerinţele existente, fără modificări. Diferite ţări au tradiţii, perspective şi cerinţe de reglementare pentru managementul actelor diferite. În unele cazuri, acestea vor trebui luate în considerare la aplicarea Specificaţiei Cerinţelor Model, mai ales atunci când se folosesc pentru a contura un nou sistem. Din acest motiv, MoReq2 permite pentru fiecare ţară a Uniunii Europene să adauge un „capitol naţional” sau „capitolul zero”, care stabileşte cerinţele naţionale cum ar fi:

- traducerea terminologiei şi conceptelor esenţiale;
- cerinţele naţionale legislative şi de reglementare;
- standardele naţionale şi liniile directoare asupra accesibilităţii
- alte eventuale cerinţe naţionale
- resursele naţionale pentru informaţii viitoare.

1.9 Adaptarea acestei Specificații

Cerinţele din această Specificaţie sunt destinate să servească doar ca model. Nu sunt obligatorii pentru toate posibilele implementări ale SMAE; unele cerinţe nu se vor aplica în anumite medii. Diversele sectoare de activitate, diferitele niveluri de implementare, diferitele tipuri de organizaţii şi alţi factori vor introduce de asemenea cerinţe suplimentare specifice.

În consecinţă, această Specificaţie trebuie să fie adaptată înainte de folosire pentru scopurile achiziției.

Adaptarea pentru achiziție ar trebui:

- să adauge sau să elimine cerinţe, aşa cum sunt ele solicitate în mod specific de către organizaţie.
- să ajusteze cerinţele astfel încât să fie făcute cât mai specifice. De pildă:
  - cerinţe care precizează unul sau mai multe rezultate pot fi schimbate pentru un singur rezultat solicitat;
  - cerinţe pentru amploare şi performanţe.
- să includă detalii specifice organizaţiei, cum ar fi mediul software
- să indice cu claritate cerinţele care sunt:
  - neschimbate din MoReq2
  - noi
  - eliminate
  - adaptate

Această Specificaţie a fost pregătită astfel încât ea să poată fi folosită în format electronic sau pe hârtie. A fost pregătită folosindu-se Microsoft Word 2003 şi este publicată în următoarele formate:

Microsoft Word 1997–2003 (versiunea 11);

Microsoft Word 2007 (versiunea 12);

Adobe PDF (versiunea 1.4)

Utilizarea în format electronic are o serie de avantaje; detalii sunt furnizate în anexa 3.

1.10. Organizarea prezentei Specificaţii

Specificaţia este organizată în capitole, care sunt împărţite în secţiuni.

Următorul capitol (capitolul 2) oferă o privire de ansamblu asupra câtorva cerinţe esenţiale, începând cu terminologia fundamentală pentru Specificaţie.

Capitolele de la 3 la 9 conţin în detaliu cerinţele funcţionale fundamentale ale unui SMAE. Fiecare capitol conţine o grupare logică de cerinţe funcţionale. Totuşi, dată fiind natura subiectului, există suprapuneri inevitabile între capitole.

Capitolul 10 este împărţit în câteva secţiuni, fiecare din ele conţinând cerinţe pentru câte un modul opţional al unui SMAE. Unele dinte aceste secţiuni (de ex. secţiunea referitoare la sistemele dispersate) pot fi esenţiale în anumite organizaţii, dar inutile în altele.

Capitolul 11 conţine cerinţe non-funcţionale.

Capitolul 12 identifică cerinţele pentru administrarea metadatelor; definițiile elementelor de metadate necesare să sprijine MoReq2 sunt menţionate în anexa 9.

Capitolul 13 conţine un model de referinţă oficial al SMAE, aşa cum este înţeles în această Specificaţie. Acest model poate fi folosit pentru a înţelege aspecte de bază ale Specificaţiei, cum ar fi definiţii oficiale a termenilor (de pildă clasă, sub-dosar, volume) şi relaţiile care există între ele (de ex. „ce poate fi stocat într-un dosar electronic?”).

Anexele conţin detalii despre documentele de referinţă şi administrative şi alte informaţii. Anexa 9 cuprinde modelul de metadate MoReq2. Acesta este publicat separat de restul MoReq2, pentru a ușura referențierea încrucișată și datorită mărimii acestuia.

Ca răspuns la cererile venite din mai multe direcţii, au fost dezvoltate materiale de testare pentru a completa aceste cerinţe. Materialele de testare sunt publicate lângă exemplarul electronic al cerinţelor. Structura MoReq2 este proiectată să suporte testarea conformităţii cu aceste cerinţe; de pildă fiecare secţiune din capitolul 10 reprezintă un modul de testare opţional. Pentru mai multe detalii asupra testării MoReq2 vezi www.DLM-Network.org.

Cerinţele sunt prezentate sub forma unui tabel, cu o singură cerinţe pentru fiecare rând dintr-un tabel. Aceasta este ilustrată în figura 1.1.

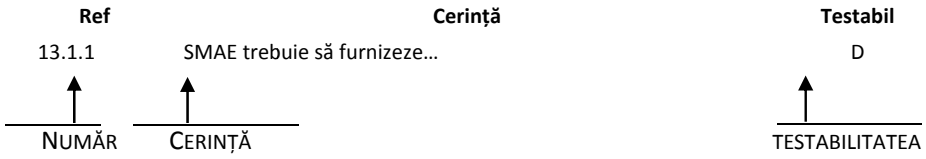


Figura 1.1

Fiecare cerinţă are un număr şi fiecare este exprimată în limbaj natural.

1.11. Testarea de conformitate

Posibilitatea de testare

Fiecare cerinţă este urmată de un atribut numit: „testabil”. Acesta indică în ce măsură va fi posibil să se testeze conformitatea cu cerinţa. Posibilele valori ale atributului „testabil” sunt descrise mai jos, cu exemple:

> **D — Cerinţa poate fi testată oficial.** Un exemplu este „Un SMAE trebuie să permită cel puţin trei niveluri ierarhice în schema de clasificare”. Aceasta poate fi testată prin încercarea de a stabili o ierarhie cu trei niveluri.
>
> **N — Cerinţa nu poate fi testată oficial.** Un exemplu este: „ SMAE trebuie să accepte schema de clasificare a activităţii organizaţiei”. Nu există nici o posibilitate de a testa universal acest lucru.
>
> **P — Cerinţa poate fi testată, dar acoperirea testului este parţială şi/sau este posibil să fie identificată o lipsă de conformitate**. Un exemplu este: „ SMAE nu ar trebui să limiteze numărul de niveluri în ierarhie”. Nu există nici o posibilitate, oficială pentru a testa lipsa unei limite. Totuşi, se consideră că cerinţa este testabilă cu acoperire parţială, de pildă prin testare pentru un număr mare de niveluri; în timpul testării este posibil ca o limită a numărului de niveluri ar putea fi observată, indicând faptul că SMAE nu se conformează cerinţei.

Sistemele de sprijin ale SMAE

Această Specificaţie este însoţită de Cadrul de testare MoReq2. Acest cadru oferă documentaţia care permite să fie testată conformitatea unui SMAE cu cerinţele MoReq2.

Câteva cerinţe MoReq2 se bazează pe elementele de hardware şi software care nu sunt elemente ale SMAE. De pildă, MoReq2 include:

- cerinţe referitoare la integrarea e-mail-urilor, care se bazează pe caracteristicile clientului de e-mail.
- cerinţe de integritate şi scalabilitate, care se bazează pe caracteristicile software-ului de management al bazei de date;
- cerinţe de scanare, care se bazează pe programul de scanare.

Evident, este imposibilă testarea oricărui SMAE cu toate elementele de hardware şi software care ar putea fi folosite. Prin urmare, şi este o problemă de definire, asemenea cerinţe vor fi testate cu o combinaţie de componente software şi hardware specificată de furnizorul SMAE. Certificatul rezultat în urma testării de conformitate va specifica ce componente software şi hardware au fost folosite pentru testare; conformitatea va acoperi doar acel mediu specificat. Pentru potenţialii utilizatori ai SMAE care doresc să identifice nivelul de conformitatea cu orice alt software şi/sau hardware, informaţia va trebui obţinută de la caz la caz.

1.12. Cerinţe obligatorii şi cerinţe recomandabile

MoReq2 conţine atât cerinţe obligatorii, cât şi cerinţe opţionale. Acest nivel de obligativitate este indicat după cum urmează:

- cuvântul „trebuie” indică faptul că cerinţa este obligatorie;
- cuvântul „ar trebui” indică faptul că cerinţa este recomandabilă.

În toate cazurile, nivelul de obligativitate este dependent de context. Aşadar, de pildă, o cerinţă obligatorie într-un modul opţional este obligatorie doar în contextul acelui modul opţional.

În unele cazuri, o cerinţă este obligatorie doar dacă o cerinţă recomandabilă este îndeplinită. Acest lucru este întotdeauna clar din context; de exemplu, următoarea situaţie:

- 3.1.17: SMAE ar trebui să accepte exportul schemei de clasificare, în parte sau integral.
- 3.1.18: Acolo unde SMAE suportă exportul schemei de clasificare, în parte sau integral (ca în 3.1.17), acesta trebuie să includă metadatele asociate […]

semnifică faptul că funcţionalitatea cerută de 3.1.18 este obligatorie doar dacă este furnizată funcţionalitatea recomandată impusă de 3.1.17.

1.13. Comentarii asupra prezentei Specificaţii

Informaţii despre cum se pot transmite comentarii şi observaţii pot fi găsite pe site-ul Forumului DLM: www.DLM-network.org.

2. Privire generală asupra cerinţelor SMAE

Acest capitol începe prin definirea câtorva termeni esenţiali (secţiunea 2.1.). Urmează o descriere narativă a câtorva concepte esenţiale(secţiunea 2.2) şi a diagramei entitate-relaţie a modelului pe care se bazează Specificaţia (secţiunea 2.3.).

2.1. Terminologia esenţială

MoReq2 cere ca anumiţi termeni să aibă semnificaţii precise. Ori de câte ori este posibil, aceste semnificaţii se conformează sensului uzual sau întrebuinţării generale în comunitatea *records management*-ului. Totuşi, în unele cazuri, întrebuinţarea este specifică pentru MoReq2. Toţi termenii sunt definiţi în glosar (secţiunea 13.1); câţiva termeni esenţiali sunt selectaţi din glosar şi reproduşi aici, pentru o referențiere mai facilă. Definițiile reproduse aici sunt identice cu cele din glosarul integral. În definiţiile de mai jos, termenii în italic sunt definiţi în glosar, secţiunea 13.1.

captură (verb)

(1) Actul înregistrării sau salvării unei anumite reprezentări a unui document digital (sursă:Baza de date terminologică a proiectului InterPares 2)

(2) Salvarea informaţiei într-un sistem de computere.

Notă: în contextul MoReq2, *captura actelor* este folosit pentru a denumi toate procesele implicate în introducerea unui actîn SMAE, şi anume înregistrarea, clasificarea, adăugarea de metadate şi blocarea conţinutului documentului sursă. Acest termen este folosit în general ca semnificând inserarea în SMAE şi stocarea altor informaţii, cum ar fi valori pentru metadate.

dosar de caz

Un dosar referitor la una sau mai multe operaţiuni, desfăşurate total sau parţial de o manieră structurată sau parţial-structurată, ca rezultat al unui proces concret sau al unei activităţi.

Notă: nu există o definiţie universal acceptată a acestor termeni, nici o distincţie între dosare de caz şi alte tipuri de dosare frecvent administrate de SMAE. Definiţia este prin urmare dezvoltată pentru MoReq2 şi urmărește să uşureze înţelegerea acestuia; aplicabilitatea ei în alte situaţii nu este garantată.

Notă: documentele dintr-un dosar de caz pot fi structurate sau nestructurate. Caracteristica esenţială a dosarelor de caz este că ele rezultă dintr-un proces care este cel puţin parţial structurat şi repetabil. Exemplele includ dosare cuprinzând:

- cereri de premise

- anchete despre o activitate obișnuită
- cercetare asupra unui incident
- monitorizare periodică

Notă: în mod obişnuit, alte caracteristici ale unui dosar de caz sunt că acestea:

- prezintă o structură predictibilă pentru conţinutul lor
- sunt numeroase
- sunt structurate sau parţial structurate
- sunt folosite şi administrate în cadrul unui proces cunoscut şi pre-determinat
- este nevoie să fie păstrate pentru anumite perioade, ca rezultat al unei legi sau regulament
- poate fi deschis sau închis de lucrători (angajați), utilizatori finali sau de sistemul de procesare a datelor fără a fi nevoie de aprobarea structurii de management.

Notă: acolo unde cerinţele naţionale impun şi alte distincţii, acestea vor fi specificate în Capitolul 0.

clasă

(doar în MoReq2) Porţiunea dintr-o ierarhie reprezentată de o linie care porneşte din ierarhia *schemei de clasificare*spre toate dosarele de sub ea.

Notă: aceasta poate corespunde, în terminologia clasică, conceptelor de „clasa primară”, „grup” sau „serie” (sau sub-clasă, sub-grup, sub-serie etc.) la orice nivel al schemei de clasificare.

Notă: în MoReq2, clasă înseamnă şi toate documentele alocate unei clase.

clasificare

În *records management*, identificarea sistematică şi ordonarea activităţilor şi/sau a actelor pe categorii, în conformitate cu metode, convenţii, şi reguli procedurale structurate logic, într-un sistem de clasificare.

Sursa: ISO 15489 (vezi Anexa 7)

schemă de clasificare

(în MoReq2) ordonarea ierarhică a claselor, dosarelor, sub-dosarelor, volumelor şi documentelor.

componentă

Un flux distinct de bytes care, singur sau împreună cu alte fluxuri de bytes, formează un actsau document.

Notă: acesta nu este un termen de utilizare generală

Notă: Formula „flux distinct de bytes” este folosită pentru a descrie ceea ce în mod obişnuit este numit „fişier” [*file*] în tehnologia informaţiei; cuvântul „file” nu este folosit aici, pentru a evita confuzia cu sensul din *records management*al termenului *file* [= dosar]. Conceptul esenţial este că o „componentă” este o parte integranta a conţinutului unui act, chiar dacă el poate fi manipulat şi administrat separat.

Notă: Exemplele de componente pot include:

- un document .html şi imagini .jpeg care formează o pagină web.
- un document dintr-un procesor de texte şi o foaie de calcul, caz în care actul constă din documentul din procesorul de texte care cuprinde încorporat un hiperlink către foaia de calcul.

Notă: componentele trebuie să fie distincte, adică separate una de cealaltă, Dacă un document dintr-un procesor de texte conţine încorporată o foaie de calcul (spre deosebire de cazul în care încorporează un link către respectiva foaie de calcul), atunci foaia de calcul nu poate fi considerată o componentă; în acest caz, documentul din procesorul de texte, completat cu foaia sa de calcul încorporată, formează un act, alcătuit dintr-o singură componentă.

Notă: un mesaj de e-mail cu anexe poate fi o componentă, mai multe componente sau chiar mai multe acte, în funcţie de formatul în care este stocat:

- dacă mesajul este stocat într-un format care include corpul său şi toate anexele, atunci reprezintă o singură componentă;
- dacă anexele sunt stocate separat şi legate intern de corpul mesajului e-mail-ului, atunci fiecare anexă şi corpul mesajului reprezintă o componentă
- dacă anexele sunt stocate separat de corpul mesajului, dar nu sunt legate de acesta, atunci fiecare anexă şi corpul mesajului reprezintă câte un actseparat; buna practică recomandă ca aceste acte să fie legate manual unul de celălalt.

document

Informaţie înregistrată sau obiect care poate fi tratat ca o unitate.

Sursa: ISO 15489 (vezi Anexa 7)

Notă: un document poate fi pe hârtie, microformă, pe suport magnetic sau electronic. Poate include orice combinaţie de text, date, grafice, sunete, imagini, sau orice altă formă de informaţie. Un singur document poate consta din una sau mai multe *componente*.

Notă: documentele diferă de acte în câteva aspecte importante. MoReq2 foloseşte termenul „document” cu semnificaţia de informaţie care nu este un „act”. Cuvântul „înregistrat” din definiţie nu implica acele caracteristici ale unui *act.*

act electronic

Un act care este în format electronic.

Notă: actul poate fi în format electronic ca rezultat al creării sale prin intermediul unui software sau ca rezultat al digitalizării, de ex. prin scanare.

SMAE

Sistem de management al actelor electronice

Notă: SMAE diferă de SMDE în câteva aspecte importante. Vezi secţiunea 10.3 pentru mai multe detalii.

metadată

în contextul *records management*-ului) Date descriind contextul, conţinutul şi structura unui actşi managementul său de-a lungul timpului.

Sursă: ISO 15489 (vezi Anexa 7)

Notă: unele modele se bazează pe o perspectivă conceptuală diferită asupra metadatelor. De pildă, informaţiile din înregistrarea de auditare pot fi tratate ca fiind integral metadate. Aceste perspective alternative sunt valabile şi valoroase în contextul lor, dar nu sunt de ajutor în specificaţia funcţionalităţii sistemelor şi deci nu sunt luate în considerare aici.

act

Informaţie creată, primită sau păstrată ca mărturie şi pentru informare de către o organizaţie sau persoană, în virtutea obligaţiilor juridice sau în desfăşurarea activităţilor specifice.

Sursă: ISO 15489 (vezi Anexa 7)

Notă: definiţii naţionale pot fi aplicabile

Notă: un act poate încorpora unul sau mai multe documente (de ex. când un document are anexe) şi poate fi pe orice suport şi în orice format. În consecinţă, poate fi format din una sau mai multe *componente*. În plus faţă de conţinutul documentului(-telor), un act ar trebui să includă informaţii contextuale şi, dacă e cazul, informaţii structurale (adică informaţii care descriu conţinutul actului). O trăsătură esenţială a actului este că nu poate fi modificat.

Notă: atât *actele electronice*, cât şi un *act fizic* pot fi administrate prin intermediul unui SAME.

sub-dosar

Subdiviziune intelectuală a unui dosar

Notă: sub-dosarele sunt folosite în mediile cu management al dosarelor de caz. În mod obişnuit, fiecare sub-dosar are un nume şi fiecare sub-dosar este folosit pentru a stoca un anumit fel (sau anumite feluri) de acte pentru o etapă a unui caz, cum ar fi: „facturi”, „evaluări”, „corespondenţă”. Acestea pot fi, totuși, folosite de asemenea și în medii cu dosare generale.

volum

O subdiviziune a unui sub-dosar.

Notă: aceste subdiviziuni sunt create pentru a îmbunătăţi managementul conţinutului unui dosar, prin crearea unor unităţi care sunt prea mari pentru a fi administrate cu succes. Subdiviziunile sunt mai degrabă mecanice (de ex. bazate pe numărul de act sau secvenţe de numere sau perioade de timp) decât intelectuale.

2.2. Concepte esenţiale

Conceptele esenţiale cerute pentru înţelegerea acestei Specificaţii sunt:

- act şi act electronic
- act cu autoritate
- dosar electronic, sub-dosar şi volum
- schemă de clasificare
- clasă
- SMAE
- captură de act
- roluri de utilizator

act şi act electronic

După cum este explicat în secțiunea 2.4 a Liniilor directoare ale Forumului DLM (anexa 1), actele constau din:

- conţinut
- structură
- context
- prezentare

Conţinutul este prezent în unul sau mai multe documente fizice şi/sau electronice, care conţin mesajul (conţinutul informaţional) al actului. Acestea sunt astfel stocate încât viitorii utilizatori să le poată înţelege, pe ele şi contextul lor. Aceasta presupune că un actconstă, în plus faţă de conţinutul documentului(elor), din informaţii despre structura şi metadatele care furnizează informaţii despre contextul lor. Prezentarea depinde de combinaţia dintre conţinutul actului, structura şi (în cazul actelor electronice) de software-ul folosit pentru a-l reda.

În cazul documentelor fizice, marea majoritate a actelor sunt pe hârtie şi sunt incluse în dosare, constituite fizic din unul sau mai multe volume, cuprinse între coperte. Controlul de procedură ar trebui să prevină ca utilizatorii să schimbe actele sau poziţia lor în cadrul dosarului.

Un concept similar se aplică şi actelor electronice. Un act constă din unul sau mai multe documente electronice. Acestea pot fi documente din procesoare de texte, mesaje e-mail, foi de calcul, filme sau imagini, fişiere audio sau orice alt tip de obiect digital. Documentele devin acte când ele sunt reţinute, deci „capturate”, într-un SMAE. Prin captură, actele sunt „clasate”, adică le sunt atribuite coduri corespunzătoare clasei din schema de clasificare căreia ele îi aparţin,

permiţând unui SMAE să le administreze. Actele sunt în mod obişnuit repartizate într-un dosar — deşi nu întotdeauna, după cum se va vedea mai jos.

În perspectiva păstrării, este necesar să ţină cont că multe acte electronice sunt la rândul lor constituite din câteva componente (cuvântul „componentă" este folosit în MoReq2 pentru a evita cuvântul IT „fişier" [*file*], astfel încât să se reducă posibilitatea unei confuzii cu conceptul de „dosar" [*file*] din *records management*). Fiecare componentă este un obiect administrat de sistemul de operare al calculatorului şi poate exista în formate diferite; dar ele toate împreună formează un act. Nu toate actele au mai mult de o componentă; de pildă, cele mai multe documente din procesoarele de texte sunt formate dintr-o singură componentă. Un exemplu de act cu mai multe componente este o pagină web cu text, imagini şi foi de stil; nu este neobişnuit pentru o pagină web să conţină o componentă.html, mai multe componente de imagini .jpeg şi o câteva componente CSS.

acte cu autoritate

ISO 15489 descrie un act cu autoritate ca fiind un act care are drept caracteristici:

- autenticitatea
- credibilitatea
- integritatea
- utilitatea.

Aşa cum este explicat în ISO 15489, scopul oricărui sistem de *records management* ar trebui să fie cel de a se asigura că actele stocate în cadrul acestuia au autoritate. Rezumând, un act cu autoritate

- poate să demonstreze că este ceea ce se presupune a fi,
- poate să demonstreze că a fost creat sau trimis de persoana care se presupune că l-a creat sau trimis
- poate să demonstreze că a fost creat sau trimis la momentul presupus că a fost trimis
- că se poate avea încredere în el, deoarece se poate avea încredere în conţinutul său că este o reprezentare completă şi precisă a operaţiunilor, activităţilor sau faptelor pe care le atestă;
- este complet şi neschimbat
- poate fi localizat, regăsit, prezentat şi interpretat.

Cerinţele din MoReq2 sunt proiectate să se asigure că actele stocate într-un SMAE conform MoReq2 au autoritate. Totuşi, doar conformitatea cu aceste cerinţe nu este suficientă; existenţa şi conformitatea cu politicile organizaţie este de asemenea necesară.

dosar, sub-dosar şi volum electronic

Actele pe hârtie sunt în general adunate în dosare de hârtie, cuprinse între coperţi de hârtie. Dosarele de hârtie sunt grupate într-o structură sau schemă de clasificare. Într-un SMAE, actele electronice pot fi administrate ca şi cum ar fi adunate în dosare electronice şi stocate între

„coperţi” electronice. În fapt, dosarele şi coperţile electronice nu au o existenţă reală; ele sunt virtuale, în sensul că ele nu conţin în realitate nimic; de fapt, ele constau din atribute de metadate ale actelor atribuite lor. Mai departe, în multe cazuri nu este nevoie să existe o reală distincţie în sistemele electronice între dosare [conținut] şi coperte. Totuşi, aceste detalii nu sunt vizibile utilizatorului SMAE; softul de aplicaţie SMAE permite utilizatorilor să vizualizeze şi să administreze coperţile ca şi cum ele ar conţine fizic documente destinate logic să aparţină unui anume dosar. Această perspectivă centrată pe utilizator va fi urmată în această Specificaţie. Prin urmare restul Specificaţiei va descrie dosarele electronice ca şi cum ar „conţine” acte, pentru uşurinţa de înţelegere. Este de observat, totuşi, că deşi această Specificaţie oferă cerinţe funcţionale pentru administrarea dosarelor electronice, nu indică maniera în care conceptul de „dosar” este implementat.

În unele medii, este util să se împartă dosarul în sub-dosare. Divizarea în sub dosare este una de natură „intelectuală”, adică (în general) ea solicită intervenţia umană pentru a decide în care sub-dosar ar trebui să fie stocat un act. Sub-dosarele sunt adesea folosite în mediile cu prelucrare pe cazuri. Un exemplu ar fi un dosar de vânzare al unui teren, cu sub-dosare pentru fiecare activitate implicată în vânzare (cum ar fi reclame, contracte, relaţiile cu avocaţii etc.)

Un sub-dosar este prin urmare o diviziune a unui dosar pe baza tipului de conţinut, spre deosebire de, cum se întâmplă în cazul volumului, diviziunea pe baza datei actelor sau pe baza numărului de acte din dosar. În consecinţă, un sub-dosar poate fi folosit pentru a permite programului să aplice diferite programări de reţinere şi dispoziţie unui grup de acte dintr-un dosar.

Indiferent dacă sub-dosarele sunt folosite sau nu, dosarele sunt uneori divizate „mecanic” în volume de dosar, în conformitate cu nişte convenţii predefinite. Termenul „mecanic” presupune simpla aderare la aceste convenţii, care nu sunt bazate pe conţinutul intelectual al dosarelor, ci pe mărimea sau numărul de acte conţinut în el sau perioada de timp cuprinsă. Această practică îşi are originea în sistemul dosarelor de hârtie, cu scopul de a le restrânge la nişte mărimi administrabile. Ea poate fi continuată şi în cazul dosarelor electronice, pentru a le limita la nişte mărimi administrabile, pentru evaluare, transfer sau ale scopuri de administrare. Este în mod special potrivită pentru administrarea dosarelor care sunt deschise o lungă perioadă de timp, şi/sau care ajung să aibă un număr mare de acte.

Deşi distincţia între dosare şi volume de dosare este clară, implicaţiile sunt mai puţin limpezi. Şi aceasta deoarece implicaţiile deciziei de a împărţi un dosar în volume pot varia în conformitate cu nevoile de implementare. Aceste variaţii decurg din:

- unele dosare sunt închise după o perioadă, şi deci unitatea folosită pentru scopuri administrative este dosarul (chiar dacă un dosar constă din mai multe volume). Exemple ar putea fi un dosar cu o mică afacere sau dosarul unui proiect.
- unele dosare au o perioadă de lucru nelimitată (sau aproape nelimitată) şi astfel unitatea folosită pentru scopuri administrative este volumul. Exemple ar putea fi un dosar de acte despre o regiune geografică sau un dosar care se ocupă de un subiect care este independent de timp, cum ar fi unele politici, sau un dosar de facturi unde un nou volum începe în fiecare an.

În cazuri relativ rare, actele pot fi stocate şi în afara unui dosar — prin repartizarea într-o clasă. Această situaţie este explicată 3.2.17.

Schema de clasificare

Records management-ul alcătuiește dosarele într-o manieră structurată şi buna practică dictează ca această structură să fie reflectarea funcţiilor activităţii. Reprezentarea acestei alcătuiri este definită drept „schema de clasificare”. Schema de clasificare este în mod obişnuit o ierarhie. În cele ce urmează, MoReq2 se concentrează pe perspectiva ierarhică; alte abordări nu privesc MoReq2, iar o ordonare ierarhică este o pre-condiţie a conformării cu MoReq2

Aşa cum dosarele par să existe chiar dacă ele nu sunt altceva decât grupări de acte, la fel şi nivelurile superioare ale ierarhiei schemei de clasificare par să existe, deşi ele nu sunt altceva decât grupări de dosare şi/sau de niveluri inferioare. Cât despre dosare, Specificaţia stabileşte cerinţe pentru ierarhie fără să impună o manieră în care aceasta să fie implementată.

Dosarele pot apărea la orice nivel al ierarhiei. Aceasta este ilustrată în figura următoare, care reprezintă o schemă de clasificare imaginară, care înfățișează clasele şi dosarele alocate clasei de la cel mai scăzut nivel. Schema imaginară este mult mai simplă decât o schemă de clasificare reală.

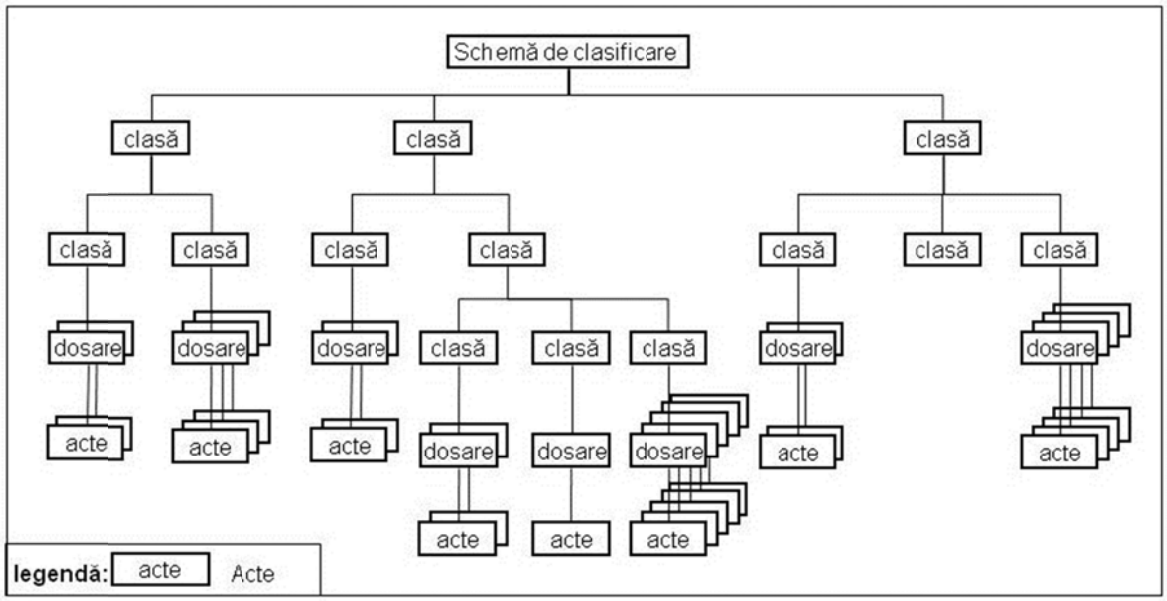


Figura 2.1

De remarcat că figura de mai sus este destinată doar prezentării posibilelor relaţii selectate între niveluri, dosare, şi acte. Nu prezintă toate posibilele niveluri sau toate posibilele ordonări.

clasă

MoReq2 foloseşte termenul „clasă” pentru a descrie o porţiune a ierarhiei reprezentată de o linie care porneşte din orice punct al ierarhiei către toate dosarele de sub ea. Termenul clasă corespunde prin urmare unui „grup” sau „serii” (sau sub-grup sau sub-serie) din anumite lucrări.

Vizual, o clasă a ierarhiei corespunde unei ramuri de copac. O clasă poate astfel să conţină alte clase, aşa cum o serie conţine sub-serii sau sub-sub serii. Continuând cu exemplul de mai sus, casetele umbrite şi liniile groase din următoarea diagramă sunt un exemplu de clasă.

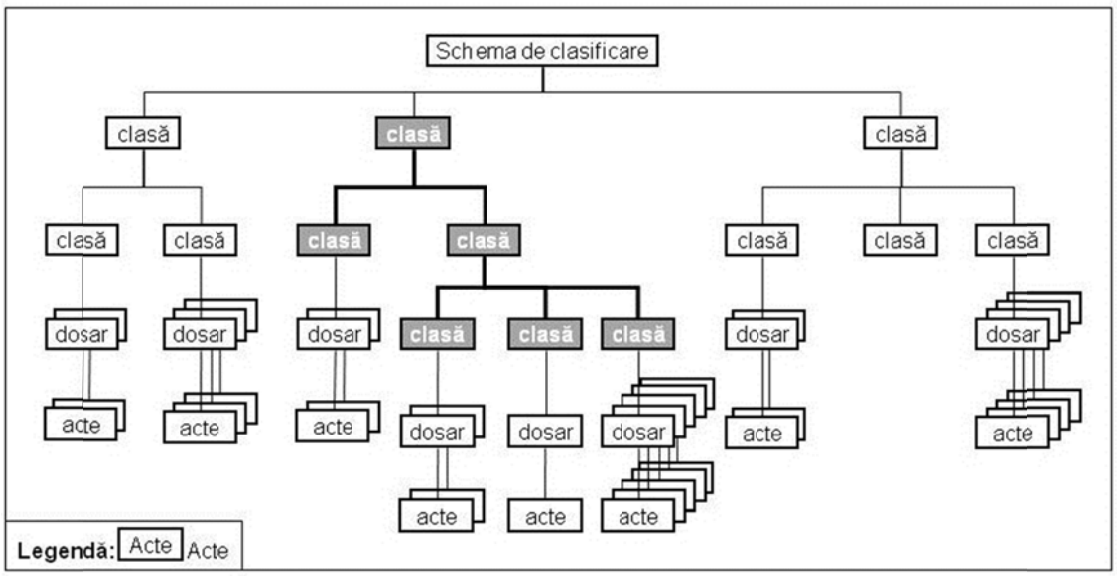


Figura 2.2

MoReq2 foloseşte de asemenea termenul „clasă” pentru a defini totalitatea dosarelor, actelor etc., atribuite unei clase — aşa cum termenul „sticlă” defineşte atât recipientul, cât şi conţinutul de lichid. Acest dublu sens este intenţionat şi interpretarea potrivită a termenului este întotdeauna clară din context.

MoReq2 foloseşte termenii de „fiică” şi „mamă” pentru a descrie relaţiile dintre entităţi. O „fiică” a unei entităţi este o entitate care este sub ea în ierarhie (altfel spus, o entitate descendentă). O „mamă” este o entitate care este o entitate care se află situată deasupra în ierarhie. Deci, ca exemplu, fiicele unei clase pot fi clase, dosare şi (în cazuri rare) acte.

MoReq2 permite ca actele să fie atribuite sau stocate direct într-o clasă fără a fi într-un dosar. Această situație apare în cazuri relativ rare, aşa cum apare descris în MoReq2.

sistem de management al actelor electronice (SMAE)

Un SMAE este în primul rând o aplicaţie pentru managementul actelor electronice, deşi el poate fi de asemene folosit pentru a administra acte fizice.

Un SMAE este adesea integrat cu un Sistem de administrare a documentelor electronice (SMDE) sau cu alte aplicaţii tip *business*. Tehnic, un SMAE administrează acte, în timp ce un SMDE administrează documente (care nu sunt acte). Totuşi, în special când sunt folosite pentru a sprijini activitatea de zi cu zi, funcționalitatea lor poate fi dificil de separat. Acest aspect este dezvoltat pe larg în secţiunea 10.3, care se referă la aspectele de management al documentelor.

captura actelor

Documentele produse sau primite în cursul desfăşurării activităţii devin acte când ele sunt puse spre păstrare, respectiv „capturate”, într-un SMAE. În timpul capturii, actele sunt „clasate”, adică le sunt atribuite coduri corespunzătoare clasei căreia îi aparţin, permiţând SMAE să le administreze; de asemenea, le atribuie și un identificator unic.

În multe cazuri, documentele care sunt puse de-o parte sau capturate, devin acte prin legarea lor de un anume proces al activităţii, aşa cum frecvent se întâmplă în fluxul de lucru. De pildă, când o factură este ridicată, ea ar trebui automat să genereze un act care să fie capturat. În alte cazuri, poate exista o politică ca fiecare documente referitor la activitate să devină un act, chiar dacă nu participă oficial în acel proces al activităţii. Totuşi, în alte situaţii, procesul de captură va fi iniţiat selectiv de utilizator. Stabilirea acelor documente care ar trebui capturate într-un sistem de acte ar trebui să se bazeze pe analiza mediului de reglementare, pe cerinţele de afaceri şi de responsabilitate şi pe riscul implicat de ne-captura actelor. Un exemplu este o înştiinţare dintr-o organizaţie, care se referă la aspecte de politică; organizaţia poate stabili că doar înştiinţările care sunt semnificative vor fi declarate acte (adică înştiinţările nesemnificative, cum ar fi cele referitoare la organizarea întâlnirilor, nu vor constitui, în general, acte). În anumite situaţii, proiectele vor putea fi considerate semnificative şi vor deveni acte, în timp ce în alte situaţii proiectele nu vor deveni acte. MoReq2 urmărește să acopere oricare din aceste scenarii. Altfel spus, MoReq2 descrie un sistem de tip „office” pentru utilizare generală, nu doar un sistem de *records management* pentru un anumit tip de aplicații sau pentru uzul exclusiv al arhiviştilor sau administratorilor.

roluri de utilizatori şi roluri de administrator

MoReq2 foloseşte conceptul de „utilizator” în sensul oricărei persoane care are o permisiune validă de a lucra folosind SMAE. Prin urmare, oricine care are permisiunea de a se loga la un SMAE este un utilizator, inclusiv administratorii. Cu toate acestea, distincţia între administratori şi alţi utilizatori poate fi complexă şi, uneori, neclară. MoReq2 prin urmare foloseşte conceptul de „roluri” în definirea mai multor cerinţe.

Diferitele organizaţii vor implementa diferit un SMAE. De pildă, o mică organizaţie poate implementa un SMAE cu un singur administrator, în timp ce o organizaţie largă poate avea nevoie de câteva poziţii administrative, fiecare cu diverse permisiuni de acces. Din acest motiv, nu este utilă identificarea profilurilor specifice de acces în această Specificaţie generică; ca abordare alternativă, MoReq2 foloseşte conceptul de „roluri”.

MoReq2 identifică 2 tipuri de roluri: „roluri de utilizator” şi „roluri de administrator”. În practică, cele mai multe organizaţii vor avea mai mult de o persoană în astfel de roluri; şi multe organizaţii vor defini alte roluri. Exemplificări de roluri cu posibile permisiuni de acces sunt schiţate în matricea din la capitolul 13.4.

Pe scurt, totuşi, un „rol” în MoReq2 este ceva asemănător unui profil de utilizator — nu este o slujbă sau un post, ci un set de responsabilităţi şi permisiuni funcţionale împărţite între câţiva utilizatori. MoReq2 cunoaşte exemple de 2 administratori şi 2 roluri de utilizatori.

Rolurile de administrator acţionează în sensul administrării actelor înseşi; interesul lor este managementul actelor ca entităţi şi nu a conţinutului sau a contextului de activitate. Ele administrează de asemenea hardware, software şi stocarea SMAE, asigură realizarea de copii de siguranță şi administrează performanţele unui SMAE.

Spre deosebire de rolurile de administrator, rolurile de utilizatori au acces la capacităţile de care un lucrător de birou sau un cercetător are nevoie atunci când utilizează un act. Aceasta include adăugarea de documente, căutarea şi regăsirea actelor; interesul lor este în primul rând orientat

spre conţinutul actelor şi nu spre administrarea lor — cu alte cuvinte, ei sunt interesaţi de procesele de activitate oglindite în acte.

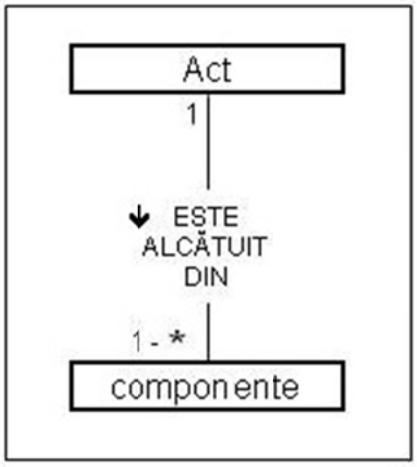
2.3. Modelul entitate-relaţie

Această secţiune conţine un model entitate-relaţie care poate fi folosit ca un ajutor pentru înţelegerea Specificaţiei. Secţiunea 13.3 conţine şi o explicare narativă.

Un aspect important al diagramei este că nu e nevoie să reprezinte structuri reale stocate în SMAE. Ea reprezintă o viziune teoretică a entităţilor asociate cu actele. Un SMAE foloseşte aceste relaţii pentru a produce un comportament echivalent cu structurile din diagramă. Vezi secţiunea 2.2. pentru mai multe explicaţii asupra acestui punct.

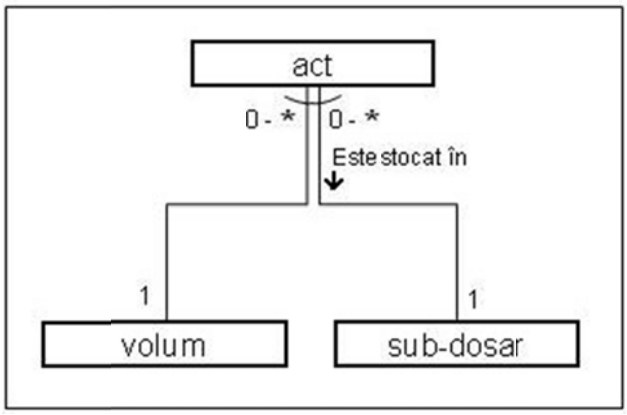
Relaţiile între dosare, volume, acte şi alte entităţi importante sunt descrise în diagrama entitate-relaţie care urmează. Aceasta este o reprezentare formală a structurilor selectate care pot fi folosite pentru a descrie comportamentul unui SMAE.

În această diagramă, entităţile — dosare, acte etc. — sunt reprezentate de dreptunghiuri. Liniile care le unesc reprezintă relaţiile dintre entităţi. Fiecare relaţie este descrisă prin textul din mijlocul liniei; şi acesta ar trebui să fie citit în direcţia săgeţii. Fiecare capăt al relaţiei are un număr, care reprezintă numărul apariţiei (strict, cardinal); numerele sunt explicate în legendă. Deci, pentru exemplificare, figura 2.3 înseamnă: „un act este format din una sau mai multe componente” (de observat direcţia săgeţii relaţiei).



Figură 2.3

O linie curbă care traversează una sau mai multe relaţii indică faptul că relaţiile sunt reciproc excluse, pentru orice situaţie dată. Deci, de pildă, linia curbă din figura 2.4 înseamnă ,,fiecare act este stocat fie într-un volum, fie într-un sub-dosar, dar nu în amândouă”.



Figură 2.4

De observat că entitatea Clasă se referă la ea însăşi prin relaţia „este compusă din”. Această relaţie descrie, în termeni formali, relaţia între clase într-o schemă ierarhică de clasificare, unde o Clasă poate fi formată din una sau mai multe Clase. Dacă această relaţie (uneori numită o relaţie recursivă) este înlăturată, modelul se aplică în egală măsură şi relațiilor non-ierarhice.

În continuarea textului MoReq2, termenii tipăriţi cu litere aldine albastre indică prima întrebuinţare a termenului definit în glosar. În versiunea electronică, aceasta este un hiperlink spre definiţie, astfel încât apăsarea CTRL + clic pe termen permite navigarea către definiţia din glosar, iar apăsarea CTRL + clic pe definiţia din glosar conduce la navigarea înapoi la termen.

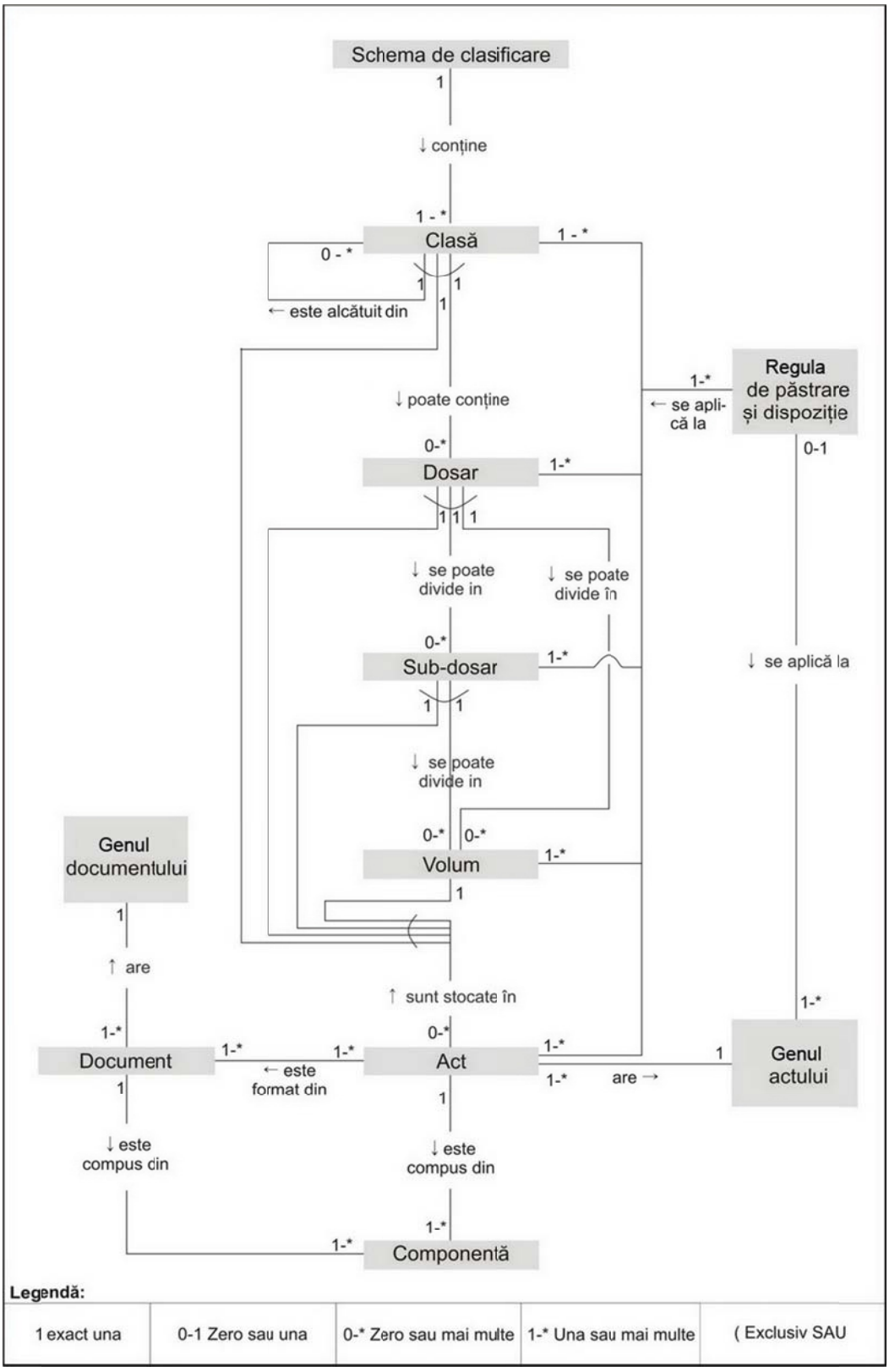

Schema de clasificare
1
↓ conține
1 - *
Clasă
0 - *
1
1
1
1
← este alcătuit din
1 - *
Regula de păstrare și dispoziție
1-*
← se aplică la
0-1
↓ poate conține
0-*
Dosar
1-*
1
1
1
↓ se poate divide in
↓ se poate divide în
0-*
Sub-dosar
1-*
↓ se aplică la
1
1
↓ se poate divide in
0-*
0-*
Genul documentului
Volum
1-*
1
1
↑ are
↑ sunt stocate în
1-*
0-*
1-*
Document
1-*
1-*
← este format din
Act
1-*
1
Genul actului
1
1-*
are →
1
↓ este compus din
↓ este compus din
1-*
1-*
Componentă
Legendă:
1 exact una
0-1 Zero sau una
0-* Zero sau mai multe
1-* Una sau mai multe
(Exclusiv SAU

Figura 2.5

3. Schema de clasificare și organizare dosarelor

Acest capitol prezintă cerinţele pentru administrarea schemei de clasificare şi a organizării dosarelor. Mai întâi, prezintă cerinţele pentru stabilirea unei scheme de clasificare în secţiunea 3.1. Apoi, prezintă cerinţe relativ la clase şi dosare (secţiunea 3.2) şi volume şi sub-dosare (secţiunea 3.3). Secţiunea 3.4 prezintă cerinţele asociate cu mentenanţa schemei de clasificare şi secţiunea 3.5 acoperă probleme de parcurgere a schemei. `

O schemă de clasificare este fundamentul pentru orice SMAE, aşa cum este descris în detaliu în secţiunea 2.2. Ea permite unui act electronic să fie stocat împreună cu alte acte care îi furnizează contextul, definind maniera în care actele electronice vor fi grupate în dosare electronice şi relaţiile dintre dosare.

O diferenţă semnificativă între MoReq2 şi predecesorul său este că MoReq2 permite declararea unui act atât direct într-o clasă, cât şi într-un dosar. MoReq-ul iniţial nu permitea declararea directă într-o clasă, ci doar într-un dosar.

MoReq2 permite astfel ca un act să fie capturat într-unul din următoarele niveluri:

- clasă
- dosar
- sub file
- volum

Această situaţie este prezentată în diagrama următoare, care adaugă asemenea acte (umbrite) imaginii din secţiunea 2.1.

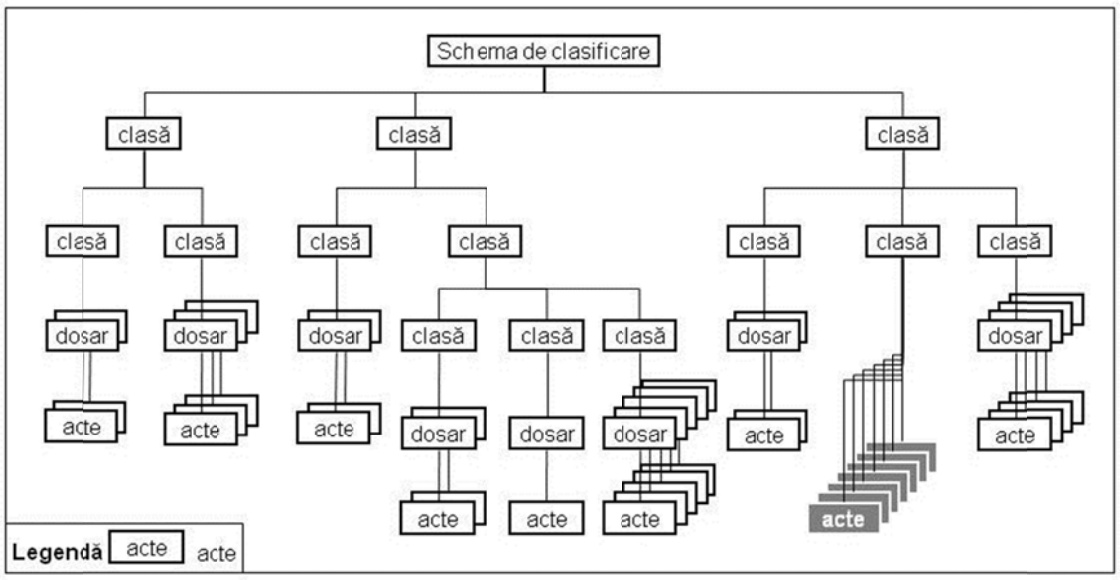


Figura 3.1

Această schimbare a fost introdusă în primul rând pentru a reflecta cerinţele sistemelor cu mare volum de tip management de caz. De pildă, un mare număr de acte, cum ar fi cereri de permise, pot fi atribuite direct unei clase, fără nevoia de a mai deschide dosare.

Totuşi, această schimbare nu înseamnă că se renunţă la nevoia unei scheme de clasificare ierarhice, sau (în cele mai multe cazuri) la existenţa dosarelor. Înseamnă mai degrabă că există situaţii speciale (cum ar fi documentaţia simplă de caz în cantităţi mari). Folosirea nepotrivită a acestei caracteristici va induce riscul unor dificultăţi ulterioare în managementul documentelor şi utilizatorii MoReq2 sunt sfătuiţi să folosească această funcţionalitate doar după o atentă analiză. Este puţin probabil ca cei mai mulţi utilizatori de MoReq2 să folosească această funcţionalitate şi de aceea MoReq2 include cerinţa ca această funcţionalitate să poată fi dezactivată.

Conformitatea cu MoReq2 presupune suport pentru clasificarea ierarhică. Motivele sunt:

- schemele ierarhice pot asigura o organizare efectivă, stabilă şi clară a organizării actelor
- schemele ierarhice sunt cele mai frecvent folosite în Europa.

Se menţine, de asemenea, compatibilitatea cu versiunea anterioară de MoReq2. Mai multe cerinţe folosesc conceptul de clasă. În multe cazuri, poate fi posibil să se aplice cerinţele unei scheme de clasificare non-ierarhice; dar acest lucru nu este întotdeauna posibil.

Este esenţial ca schema de clasificare (tehnic vorbind, o schemă de clasificare a actelor) să fie strict aliniată cu nevoile de activitate ale organizaţiei. Buna practică sugerează că organizaţia identifică o schemă de clasificare a activităţilor înainte de a proiecta o schemă de clasificare a actelor,.

3.1. Configurarea schemei de clasificare

Ref	Cerinţă	Testabil
3.1.1.	Un SMAE trebuie să accepte şi să fie compatibil cu schema de clasificare a activităţilor unei organizaţii.	N

Ref	Cerinţă	Testabil
	Această cerinţă nu este testabilă în majoritatea cazurilor; este inclusă ca o subliniere pentru utilizatorii MoReq2 a necesităţii de a alinia schema de clasificare folosită de MoReq2 cu nevoile de activitate ale organizaţiei. Aceste nevoi ar trebui să fie reflectate de ordonarea actelor în afara SMAE	
3.1.2.	Un SMAE trebuie să menţină integritatea internă (integritatea relaţională şi altele asemenea) oricând, indiferent de: ▪ menţinea activităţilor ▪ alte acţiuni ale utilizatorilor ▪ defecţiuni ale componentelor sistemului *Altfel spus, trebuie să fie imposibil să apară o situaţie, atunci când se produc acţiuni ale unui utilizator sau defecţiuni ale sistemului, care să genereze probleme cu SMAE sau cu baza lui de date.*	P
3.1.3.	Un SMAE trebuie să permită rolurilor de administrator să atribuie fiecărei scheme de clasificare un identificator, titlu şi o descriere. *Aceste metadate vor accepta funcţii cum ar fi exportul schemei de clasificare şi al actelor.*	D
3.1.4.	SMAE trebuie să poată accepta o schemă de clasificare care reprezentă dosarele şi actele ca fiind organizată într-o ierarhie de clase. *Utilizarea unei scheme de clasificare ierarhice este obligatorie pentru conformitatea cu MoReq2.* *Suportul pentru minim trei niveluri reprezintă o cerinţă minimă; mai multe niveluri pot fi necesare în multe medii.*	D
3.1.5.	SMAE trebuie să permită administrarea schemei de clasificare doar prin rolul de administrator, conform cerinţei 3.1.6 *În această cerinţă, „administrare” se referă la schema de clasificare descrisă în secţiunea 3.1 şi în secţiunea 3.4.*	D
3.1.6.	SMAE ar trebui să permită administrarea claselor individuale de către rolurile de utilizator specificate şi/sau de către un grup de utilizatori specificat. *În cerinţa de mai sus, „administrare” are acelaşi sens ca în cerinţa 3.1.5. Aceasta este dorită pentru două setări:* ▪ *schemele de clasificare care sunt prea mari pentru a fi păstrare centralizat (şi care prin urmare au o administrare centralizată pentru nivelurile superioare şi o administrare descentralizată*	D

Ref	Cerinţă	Testabil
	pentru nivelurile inferioare); ▪ *schemele de clasificare care includ clasele pentru administrarea dosarelor de caz, care trebuie administrate în structura de activitate care se ocupă de caz prin alocarea de drepturi utilizatorilor autorizaţi.*	
3.1.7.	Un SMAE nu ar trebui să limiteze numărul de niveluri în ierarhia schemei de clasificare *În majoritatea setărilor, este puţin probabil ca numărul de niveluri necesare să fie mai mare de 10.*	P
3.1.8.	Un SMAE trebuie să accepte crearea unei scheme de clasificare la momentul configurării sistemului în pregătirea capturării şi/sau importării actelor electronice. *Această cerinţă urmărește să permită unei scheme de clasificare să fie pregătită în timp ce SMAE este configurat şi înainte ca el să fie folosit pentru managementul actelor.*	D
3.1.9.	UN SMAE trebuie să permită mecanismului(elor) de denumire să fie definit de către un rol de administrator în momentul configurării.	D
3.1.10.	Un SMAE ar trebui să permită introducerea notelor tip text pentru explicarea ariei de aplicare (cunoscute de asemenea ca descriptori) pentru toate clasele şi dosarele. *Notele asupra ariei de aplicare sunt explicaţii menite să clarifice conţinutul intenţionat şi/sau de evitat ale claselor şi dosarelor, pentru ajutorarea utilizatorilor.*	D
3.1.11.	Dacă o schemă oficială XML pentru MoReq2 a fost publicată, SMAE trebuie să poată importa şi exporta acte într-o formă conformă cu acea schemă.	D
3.1.12.	SMAE trebuie să suporte importul unei scheme de clasificare, în întregime sau în parte, în momentul configurării sistemului sau în orice alt moment. *Această cerinţă urmărește să permită ca o schemă de clasificare să fie pregătită în timp ce SMAE este configurat, implementat şi înainte de a fi folosit pentru managementul actelor. Acolo unde părţi sunt importate, acestea pot fi adăugate la schema existentă sau pentru a crea o nouă schemă de clasificare, dacă nu există nici una.*	D
3.1.13.	Atunci când SMAE acceptă importul parţial sau integral al schemei de clasificare, trebuie să permită importul metadatelor asociate, programării de păstrare și dispoziție şi evidența de auditare, dacă acestea există.	D

Ref	Cerinţă	Testabil
	În situaţia ideală, schema de clasificare importată va avea metadate la nivel de clasă şi termene de păstrare. În alte cazuri, acestea ar putea fi absente sau incomplete.	
3.1.14.	Atunci când SMAE importă metadatele unei scheme de clasificare, el trebuie să respingă orice clasă fără un titlu şi să creeze un raport de exceptare pentru rolul de administrator, listând clasele care au fost respinse. *Într-un SMAE care nu este conform MoReq2, poate fi posibil ca o clasă să nu aibă titlu (valoare nulă); dar o astfel de clasă va fi imposibil de utilizat în cadrul unui SMAE conform MoReq2.*	D
3.1.15.	Acolo unde SMAE importă metadatele unei scheme de clasificare, SMAE trebuie să atribuie fiecărei clase importate un cod ierarhic în una din următoarele modalităţi, conform opţiunilor setate de rolul de administrator: ▪ urmând aceleaşi reguli ca şi cum ar fi fost creată manual o schemă de clasificare; ▪ păstrând codurile originale în integralitatea lor (posibilă doar dacă structurile sunt compatibile); ▪ alăturarea codurilor originale la codurile din schema primitoare. *Dacă o ierarhie care este importată include deja coduri pentru clasele ierarhice (de pildă 4/6/4) s-ar putea ca acestea să nu mai poată fi folosite, ca şi coduri în SMAE, deoarece consecvența şi unicitatea nu pot fi garantate.* *Există mai multe posibile scenarii pentru un astfel de import, cu diferite feluri de incompatibilităţi între schemele de numerotare ierarhică. MoReq2 nu stabileşte rezultatul unei încercări de a selecta o opţiune care este logic imposibilă, deoarece schemele sunt incompatibile.* *Dacă nişte coduri existente nu pot fi utilizate, ele pot fi tratate după cum impune situaţia, de pildă, copiindu-le într-un element de metadate numit „vechiul cod al clasei”.*	P
3.1.16.	Atunci când SMAE importă metadatele şi termenele de păstrare ale unei scheme de clasificare, el trebuie să le valideze folosind aceleaşi reguli care ar fi folosite pentru crearea manuală a schemei de clasificare (vezi capitolul 12). Atunci când procesul de validare găseşte erori (de pildă, absenţa metadatelor obligatorii sau erori de format), el trebuie să le aducă în atenţia rolului de administrator care desfăşoară operaţiunea de import, identificând şi metadatele implicate. *În cazurile ideale, schema de clasificare care este importată va avea metadate (de ex., metadate pentru clasele sale) care vor fi conforme în totalitate cu*	D

Ref	Cerinţă	Testabil
	modelul de metadate MoReq2. În alte cazuri, câteva rezultate sunt posibile; MoReq2 nu obligă la nici un rezultat. Posibilele rezultate includ: ▪ *întreaga importare este anulată şi rolul de administrator este informat asupra cauzelor anulării;* ▪ *importarea unei clase care nu are metadate conforme este anulată şi rolul de administrator este informat asupra cauzelor anulării;* ▪ *rolul de administrator este solicitat să aleagă între corectarea erorii şi anularea importării clasei afectate.* ▪ *importarea continuă chiar dacă o parte a metadatelor nu este conformă, datele neconforme fiind înlocuite de valorile implicite specificate pentru elementele afectate şi se produce un raport de eroare.* *Informarea rolului de administrator nu presupune că procesul de importare să fie în prim plan sau un proces în timp real; este suficient ca procesul să fie în fundal sau un proces în loturi (*batch*).*	
3.1.17.	Un SMAE ar trebui să accepte exportarea integrală sau parţială a schemei de clasificare.	D
3.1.18.	Atunci când SMAE acceptă exportarea integrală sau parţială a schemei de clasificare, aceasta trebuie să includă metadatele asociate, rolul de administrator având posibilitatea de a selecta ce metadate sunt exportate.	D
3.1.19.	Atunci când SMAE acceptă exportarea integrală sau parţială a schemei de clasificare, aceasta trebuie să includă toate termenele de păstrare asociate, la decizia rolului de administrator.	D
3.1.20.	Atunci când SMAE acceptă exportarea integrală sau parţială a schemei de clasificare, aceasta trebuie să includă toate evidențele de auditare sau doar pe cele selectate, selecţia fiind realizată de rolul de administrator.	D
3.1.21.	Atunci când SMAE suportă exportarea (pentru oricare din cerinţele de mai sus) el trebuie să folosească o metodă documentată integral pentru a asocia entităţile una cu alta. *Documentația metodei trebuie să definească cum sunt exprimate actele, dosarele, clasele etc. şi relaţiile lor.*	D D
3.1.22.	Atunci când SMAE suportă exportarea (pentru oricare din cerinţele de mai sus), el ar trebui să exporte informaţiile în XML sau într-un format deschis standardizat.	D
3.1.23.	Atunci când SMAE acceptă copierea integrală sau parţială a unei scheme de	D

Ref	Cerinţă	Testabil
	clasificare, aceasta trebuie să includă toate metadatele asociate.	
3.1.24.	Atunci când SMAE acceptă copierea integrală sau parţială a unei scheme de clasificare, aceasta trebuie să includă toate termenele de păstrare asociate.	D
3.1.25.	SMAE trebuie să permită rolului de administrator să adauge noi clase în orice punct în cadrul unei clase, atât timp cât nu sunt dosare stocate în acel punct. *MoReq2 nu permite dosarelor şi claselor să existe la acelaşi nivel în cadrul unei clase (altfel spus, clasele şi dosarele nu pot fi amestecate într-un singur nod al ierarhiei schemei de clasificare). Acest lucru este impus din motive de bună practică de records management.*	D
3.1.26.	SMAE ar trebui să accepte definirea şi utilizarea simultană a unor scheme de clasificare multiple. *Majoritatea organizaţiilor vor obliga să fie folosită o singură schemă de clasificare pentru clasificarea primară a tuturor dosarelor într-un SMAE. Această cerinţă permite unor dosare din SMAE să aparţină unei scheme de clasificare, în timp ce altele să aparţină altei scheme de clasificare. Acest lucru poate fi cerut, de pildă, ca urmare a fuziunii a două organizaţii sau a două grupări de acte diferite dintr-o singură organizaţie, care cer regimuri de administrare diferite.*	D

3.2 Clase şi dosare

Această secţiune prezintă cerinţele care se aplică claselor şi dosarelor.

Clasele şi dosarele sunt două grupări diferite. Clasele furnizează un cadrul intelectual pentru clasificare, în timp ce dosarele grupează documente; clasele sunt structuri de construcţie a unei scheme de clasificare; în timp ce dosarele nu. În ciuda diferenţelor majore, este de ajutor să fie prezentate la un loc câteva cerinţe, atât timp cât ele sunt comune celor două grupări.

Referinţă	Cerinţe	Testabil
3.2.1.	SMAE trebuie să accepte captura, mentenanţa şi prezentarea metadatelor pentru dosare şi clase în schema de clasificare, conform cu modelul de metadate MoReq2	D
3.2.2.	Un SMAE trebuie să limiteze posibilitatea de adăugare de metadate pentru dosare şi clase la cele stabilite în modelul de metadate MoReq2	N
3.2.3.	SMAE trebuie să furnizeze un mecanism pentru alocarea automată a codului de clasificare ierarhică (acolo unde un astfel de cod nu există deja — vezi 3.1.15) pentru fiecare clasă, dosar, sub-dosar, şi volum într-o schemă de	D

Referință	Cerințe	Testabil
	clasificare. *Vezi de asemenea 7.1.1.*	
3.2.4.	SMAE trebuie să permită rolurilor de utilizatori să aloce un titlu pentru fiecare clasă, dosar, sub-dosar şi volum electronic. *Această cerinţă se aplică pentru mediile cu dosare generale. Acolo unde este necesar un sistem de management al dosarelor de caz, o abordare de denumire alternativă este necesară. Aceasta este specificată în secţiunea 10.6*	D
3.2.5.	Trebuie să fie posibilă folosirea atât a codului de clasificare, cât şi a titlului tip text de dosar, separat sau împreună.	D
3.2.6.	Un SMAE trebuie să permită unui rol de administrator să configureze codul de clasificare în momentul configurării sau mai târziu.	D
3.2.7.	Configurarea codului de clasificare poate include: • formatul identificatorului asociat la fiecare nivel al ierarhiei, de ex. alfa-numeric; • prima valoare a acestui identificator, în fiecare clasă, de ex. 1, 1000 • intervalul care trebuie folosit între clase succesive, de ex. 1, 10 • prezenţa sau absenţa de zerouri în faţa numerelor • orice prefix global, de ex. „corporaţie” • orice extensie globală, de ex, sufix de ţară • separatorul între fiecare identificator, de ex. „/”, „-„	D
3.2.8.	SMAE trebuie să înregistreze data deschiderii sau închiderii unei clase sau a unui dosar în cadrul metadatelor unei clase sau a unui dosar. *Data deschiderii sau închideri unei clase sau a unui dosar furnizează un context important pentru actele clasate în cadrul ei. Vezi de asemenea 3.3.9.* *Atunci când o clasă sau un dosar sunt deschise, este posibil să fie capturate documente în cadrul lor. Atunci când o clasă sau un dosar sunt închise, nu mai pot fi capturate acte în ele.*	D
3.2.9.	SMAE trebuie sa înregistreze în metadatele clasei sau dosarului data creării unei noi clase, a unui nou dosar, sub-dosar sau volum. *În cazul dosarelor fizice, este posibil ca data deschiderii să preceadă data creării înregistrată în SMAE. Aceasta se poate întâmpla dacă un dosar fizic este creat şi deschis doar în format fizic, înainte de a fi creat în SMAE.* *În cazul dosarelor electronice, este posibil ca data deschiderii să preceadă data creării înregistrată în SMAE. Aceasta se poate întâmpla dacă un dosar*	D

Referință	Cerințe	Testabil
	electronic este importat în SMAE dintr-un alt sistem.	
3.2.10.	Ori de câte ori o nouă clasă sau un nou dosar sunt deschise, SMAE trebuie să includă automat în metadatele sale acele atribute care sunt moştenite, în virtutea poziţiei sale în schema de clasificare. *De pildă, dacă un dosar intitulat „Întâlniri publice" se află într-o cale ierarhică:* Dezvoltare plan regional: Consultare publică: întâlniri publice *şi un rol de administrator adaugă un nou dosar intitulat : „consultări în scris" la acelaşi nivel cu dosarul „întâlniri publice", atunci noul dosar trebuie automat să preia prefixul* Dezvoltare plan regional: Consultare publică	D
3.2.11.	SMAE trebuie să permită rolului de administrator să modifice valorile metadatelor preluate, în limitele permise de modelul de metadate MoReq2. *Valorile preluate furnizează adesea o poziţie predefinită sau inițială. Aceasta poate fi schimbată, atât timp cât schimbarea este compatibilă cu modelul de metadate.*	D
3.2.12.	Orice adăugare la aceste metadate preluate ar trebui să fie preluată implicit de către toate clasele şi dosarele fiice (subordonate).	D
3.2.13.	În plus faţă de alte cerinţe din această secţiune, SMAE ar trebui să accepte alocarea de termeni de vocabular controlat conformi cu ISO 2788 ca termeni descriptivi pentru subiect în metadatele dosarelor sau claselor.	D
3.2.14.	SMAE ar trebui să accepte alocarea de termeni dintr-un vocabular controlat conformi cu ISO 5964 ca termeni descriptivi pentru subiect în metadatele dosarelor sau claselor *Cerinţele 3.2.13 şi 3.1.14 sunt identice, având în vedere că primul se referă la un tezaur monolingv, iar al doilea la un tezaur multilingv.*	D
3.2.15.	SMAE nu trebuie să impună nici o limită efectivă pentru numărul de clase sau dosare care pot fi definite.	P
3.2.16.	SMAE ar trebui să poată exporta o listă sau un inventar al tuturor dosarelor sau al dosarelor clasificate într-o anumită clasă (precum şi clasele fiică) în format XML şi/sau în format literal (*human readable format*).	P
3.2.17.	SMAE trebuie să permită unui rol de administrator să configureze o clasă astfel încât această să poată sau să nu poată stoca direct acte.	D

Referință	Cerințe	Testabil

Altfel spus, sistemul trebuie să poată fi configurat astfel încât actele să nu fie obligatoriu clasate în dosare, sub-dosar sau volume.

3.3. Volume şi sub-dosare

Într-un sistem care păstrează acte pe hârtie, subdivizarea dosarelor mari este esenţială din motive de ergonomie şi pentru supravieţuirea fizică a coperţilor, bibliorafturilor, jachetților etc. În mod obişnuit, de exemplu, dosarele de hârtie sunt limitate la 2 cm grosime, prin realizarea de volume. Când un dosar (care în realitate este primul volum al dosarului, în ciuda faptului că la el se face referinţă ca „dosar") ajunge la dimensiunea limită — 2 cm grosime, de exemplu — se consideră că este un volum închis şi se deschide un nou volum. Acest lucru nu este adevărat şi în cazul dosarelor electronice — un dosar electronic poate în mod obişnuit să crească la aproape orice dimensiune fără asemenea dificultăţi.

Cu toate acestea, în practică, există mari beneficii în divizarea dosarelor electronice mai în volume. Aceste beneficii sunt vizibile, de pildă:

- atunci când utilizatorii lucrează la distanţă (adică peste conexiuni cu bandă îngustă sau după descărcarea actelor pe un PC portabil sau pe un dispozitiv de stocare cu o capacitate limitată);
- când dosarele nu sunt niciodată închise, pentru că (de exemplu) sunt relaționate geografic.

În mod asemănător, dosarele pe hârtie sunt adesea divizate în sub-dosare — în special în mediile de administrare a cazurilor. Aceste sub-file sunt folosite pentru a organiza conținutul dosarului, adesea pe baza genului documentar.

În mod echivalent, există câteva beneficii în divizarea dosarelor electronice în sub-file, de exemplu:

- măreşte uşurinţa navigării în cadrul dosarului
- furnizează un mijloc de administrare a actelor din acelaşi dosar, dar care au cerinţe de păstrare diferite, cum ar fi cele aflate sub incidenţa legislaţiei datelor personale.

Această secţiune include cerinţe referitoare la folosirea volumelor şi sub-dosarelor, care sunt folosite în mod obişnuit să împartă dosarele care altfel ar putea fi prea largi pentru a fi administrabile. Cu toate acestea, MoReq2 nu impune ca aceste subdiviziuni să fie folosite; cere doar ca softurile conforme MoReq2 să poată furniza această opţiune dacă este nevoie.

Sub-dosarele nu erau recunoscute în versiunea anterioară a MoReq2.

În rezumat:

- fiecare dosar conţine unul sau mai multe sub-dosare
- fiecare sub-dosar conţine unul sau mai multe volume
- volumele diferitelor sub-dosare sunt create independent
- toate sub-dosarele unui dosar deschis sunt întotdeauna deschise şi toate sub-dosarele unui dosar închis sunt întotdeauna închise.

- doar un volum poate fi deschis în fiecare sub-dosar.

Pentru mai multe detalii asupra sub-dosarelor şi volumelor, vezi secţiunea 2.2.

Ref	Cerinţe	Testabil
3.3.1.	Un rol de administrator trebuie să poată configura un SMAE, în momentul configurării sau mai târziu, pentru a anula capacitatea de a crea sub-dosare şi/sau volume în cadrul dosarelor în cadrul schemei de clasificare.	D
3.3.2.	Un rol de administrator trebuie să poată configura un SMAE, în momentul configurării sau mai târziu, pentru a permite ca doar sub-dosare să fie create în dosarele dintr-o zonă a schemei de clasificare.	D
3.3.3.	Un rol de administrator trebuie să poată configura un SMAE, în momentul configurării sau mai târziu, pentru a permite ca doar volume să fie create într-un dosar din cadrul unei clase specificate a schemei de clasificare. *Intenţia celor trei cerinţe de mai sus este să permită organizaţiilor să permită sau să împiedice folosirea sub-dosarelor şi/sau volumelor în diferite părţi ale schemei de clasificare. În timp ce utilizarea celor două aduce maximum de flexibilitate, aceasta aduce complexitate şi posibile confuzii pentru utilizatori.* *Dacă o parte a schemei de clasificare este configurată pentru a permite sub-dosare, atunci toate dosarele din aceasta trebuie să conţină cel puţin un sub-dosar. Dacă o parte a schemei de clasificare este configurată pentru a permite volume, atunci toate dosarele din aceasta trebuie să conţină cel puţin un volum.* *Prin urmare, sistemul ar trebui să rămână transparent pentru utilizatori, de pildă:* ▪ *daca un sub-dosar conţine doar un volum, se acceptă ca sub-dosarul şi volumul să nu fie distinse de utilizatorii finali* ▪ *daca un dosar conţine doar un sub-dosar care conţine la rândul său doar un volum, se acceptă ca toate trei să nu fie distinse de utilizatorii finali.* *Intenţia este de a accentua că SMAE nu are nevoie să impună utilizatorilor structura „dosar, sub-dosar, volum”. SMAE trebuie să permită folosirea de sub-dosare şi volume, în timp ce permite utilizatorilor să gândească în termeni de „dosare”, doar dacă aceasta li se potriveşte.* *Esenţa acestei cerințe este că doar utilizatorul poate vedea ceea ce este esenţial din punctul de vedere al procesului de afaceri, şi nu este împiedicat de alegeri potențial aducătoare de confuzie.*	D

Ref	Cerinţe	Testabil
3.3.4.	SMAE trebuie să accepte conceptul de volume electronice deschise şi închise după cum urmează: ▪ pot fi deschise doar cele mai recent create volume în cadrul unui sub-dosar; ▪ trebuie să fie închise toate celelalte volume în cadrul unui sub-dosar.	D
3.3.5.	SMAE trebuie să împiedice utilizatorul să adauge acte electronice la un volum închis.	
3.3.6.	SMAE trebuie să permită rolurilor de administrator să adauge un volum electronic la orice sub-dosar electronic care nu este închis. *Procesul adăugării unui nou volum constă din închiderea volumului care este deschis în prezent şi crearea unui nou volum deschis.*	D
3.3.7.	SMAE trebuie să permită rolului de administrator să adauge sub-dosare oricărui dosar electronic care nu este închis.	D
3.3.8.	SMAE trebuie să permită utilizatorilor să închidă un sub-dosar în orice moment.	D
3.3.9.	SMAE trebuie să înregistreze data deschiderii unui nou volum sau a unui sub-dosar în metadate.	D
3.3.10.	Ori de câte ori un nou volum sau sub-dosar sunt deschise, SMAE trebuie să includă automat în metadatele sale acele valori ale dosarului–mamă care sunt comune (cum e definit în modelul de metadate MoReq2). *Actele într-un volum pot fi accesate indiferent dacă volumul este deschis sau închis.*	D
3.3.11.	Ori de câte ori un volum este deschis, SMAE trebuie să îi atribuie automat un identificator care este unic în cadrul sub-dosarului mamă. *Identificatorul poate fi o simplă secvenţă de numere, începând cu 1 pentru fiecare sub-dosar.*	P
3.3.12.	SMAE trebuie să înregistreze data închiderii volumului şi dosarelor în metadatele lor.	
3.3.13.	La clasificarea unor acte, utilizatorului trebuie să i se prezinte implicit cele mai recent create volume din sub-dosarul ales.	D
3.3.14.	SMAE trebuie să permită crearea de sub-dosare multiple deschise simultan	D

Ref	Cerinţe	Testabil
	într-un dosar.	
3.3.15.	SMAE trebuie să permită unui rol de administrator să şteargă un volum gol.	D
3.3.16.	SMAE trebuie să permită unui rol de administrator să şteargă un volum gol sau şi să re-deschidă volumul anterior în sub-dosar, într-o singură acţiune, înregistrând evenimentul în evidenţa de auditare. *Această cerință este prezentă pentru a corecta o eroare care a rezultat din închiderea incorectă a volumului.*	D
3.3.17.	SMAE trebuie să permită crearea unui „şablon” de sub-dosar de către un rol de administrator pentru o anumită clasă, astfel încât şablonul să specifice ca sub-dosarul să fie create automat pentru fiecare nou dosar care este creat ulterior în acea clasă. *Aceasta este destinată în primul rând pentru mediul cu management de caz. Ca un exemplu, un şablon într-o companie de asigurări poate specifica, pentru o clasă referitoare la o poliţă de asigurare, următoarele sub-dosare: politici şi amendamente, corespondenţă internă, corespondenţă cu medici specialişti, plăţi, altă corespondenţă cu clienţii. Ca urmare, fiecare nou dosar creat în clasă va fi automat creat în aceste sub-dosare.*	D
3.3.18.	SMAE trebuie să închidă automat toate sub-dosarele dintr-un dosar ori de către ori dosarul mamă este închis.	D
3.3.19.	SMAE trebuie să permită utilizatorilor să închidă fiecare volum în parte.	D

3.4 Mentenanţa schemei de clasificare

Această secţiune începe cu cerinţe pentru reclasificarea, combinarea, divizarea şi copierea claselor (3.4.1 până la 3.4.4). Toate aceste facilităţi sunt intenţionate doar pentru cazuri excepţionale, cum ar fi fuziuni instituţionale sau alte reorganizări, sau pentru a corecta greşelile angajaţilor, sau când schema de clasificare nu se potriveşte foarte bine activităţilor. Aceste posibilităţi nu sunt destinate pentru folosire curentă, în cadrul unei scheme de clasificare bine întocmită. Cerinţele ar trebui să fie citite împreună cu prevederile de la 9.3.3. până la 9.3.4. Secţiunea se încheie cu alte cerinţe legate de mentenanţa schemei de clasificare (de la 3.4.17 până la sfârşit).

Ref	Cerinţe	Testabil
3.4.1.	SMAE trebuie să permită unui rol de administrator să repoziţioneze o clasă într-o schemă de clasificare dintr-o singură acțiune. *În acest context, termenul ,,repoziționare” înseamnă reclasificarea clasei sau dosarului, adică mutarea lor într-un alt punct al schemei de clasificare.*	D

Ref	Cerinţe	Testabil
	Repoziționarea poate fi la acelaşi nivel în schema de clasificare sau la orice alt nivel. Repoziționarea implică unele cerinţe suplimentare, care sunt descrise în continuare în această secţiune.	
3.4.2.	SMAE trebuie să permită unui rol de administrator să combine două clase dintr-o singură acțiune *În această cerinţă, termenul ,,combinare" trebuie înţeles după cum urmează:* ▪ *dacă o clasă este combinată cu o altă clasă,* ▪ *toţi subordonările şi conţinutul clasei anterioare sunt relocate astfel încât să devină subordonările şi conţinutul celei de-a doua clase;* ▪ *prima clasă este închisă.*	D
3.4.3.	SMAE trebuie să permită unui rol de administrator să dividă o clasă în două părți dintr-o singură acțiune. *În această cerinţă, termenul ,,divide" trebuie înţeles după cum urmează: dacă o clasă se divide:* ▪ *o nouă clasă este creată ca o clasă-fiică a aceleiaşi clase-mamă ce conține şi clasa divizată (ceea ce presupune toate cerinţele de creare a unei noi clase, cum ar fi captura şi preluarea de metadate);* ▪ *utilizatorul specifică un punct în conţinutul clasei care trebuie divizat;* ▪ *tot conţinutul clasei din spatele acelui punct (adică având un cod de clasificare mai mare) este relocat către nou creata clasă.* ▪ *conţinutul clasei care este divizată poate fi de orice fel de conţinut permis, respectiv clase, dosare sau acte.*	D
3.4.4.	SMAE ar trebui să permită unui rol de administrator să copieze orice clasă în interiorul schemei de clasificare dintr-o singură acțiune. *În această cerinţă, termenul ,,copie" trebuie înţeles ca semnificând crearea unei copii a clasei şi a întreg conţinutului într-un alt punct din schema de clasificare, lăsând originalul la locul său. Copia poate fi la acelaşi nivel al schemei de clasificare sau la orice alt nivel. Copia implică unele cerinţe suplimentare, care sunt descrise în continuare în această secţiune.* *Această facilitate este destinată a fi utilă în momentul multiplicării ramurilor unei scheme de clasificare, o acţiune care este uneori cerută când se proiectează o parte a unei scheme care nu se bazează pe funcţii.*	D

Ref	Cerinţe	Testabil
	Utilizarea exportului urmată de import nu va fi considerată suficient de facilă pentru a se îndeplini această cerinţă.	
3.4.5.	Dacă o clasă este repoziționată sau copiată, SMAE trebuie să se asigure că noile dosare copiate sau repoziționate și întregul lor conținut sunt reclasate cu codurile de clasificare corespunzătoare noii lor poziții din schema de clasificare. *Aceasta înseamnă că fiecare clasă, dosar, sub-dosar, volum, act şi componentă care este relocată sau copiată primeşte un nou cod de clasificare şi un cod de clasificare cu calificative complete.* *Regulile pentru alocarea de noi coduri sunt aceleaşi ca regulile care ar fi urmate la crearea de noi clase, dosare, acte etc.*	D
3.4.6.	SMAE nu trebuie să ceară unui rol de administrator care repoziționează, divide, combină sau copiază clase să desfășoare acțiuni separate de importare și exportare. *Esenţa acestei cerinţe este uşurinţa în folosire; utilizatorii nu trebuie obligaţi să execute o seriede acţiuni neasociate scopului pentru a atinge acel scop.*	D
3.4.7.	SMAE nu trebuie să permită nici o repoziționare sau copiere care ar genera o structură de date care este contrară regulilor implicite din modelul entitate relaţie MoReq2 (vezi secţiunea 13.2) sau explicite din alte cerinţe. În mod specific, nu trebuie să permită nici o repoziționare care ar putea rezulta în: ▪ stocarea oricărui sub-dosar dintr-o clasă a schemei de clasificare ce a fost configurată să nu permită sub-dosare sau volume (vezi cerinţa 3.3.1, 3.3.2, 3.3.3); ▪ stocarea oricărui act direct într-o clasă ce conţine deja dosare sau invers. ▪ stocarea oricărui dosar într-o clasă care conţine deja clase sau invers.	D
3.4.8.	SMAE trebuie să se asigure că în timpul relocării toate actele electronice rămân corect alocate clasei(lor) şi/sau dosarului(lor) care a(u) fost relocate(e); şi că orice copie a oricărui sub-dosar, volum şi dosar rămân corect relaţionate (legate).	P
3.4.9.	SMAE trebuie să se asigure că în timpul copierii, toate copiile actelor electronice rămân corect alocate noilor copii ale claselor şi/sau dosarelor şi că toate copiile oricărui sub-dosar, volum sau dosar rămân corect relaţionate.	P
3.4.10.	Dacă vreo clasă, dosar, volum, sub-dosar sau act sunt relocate sau reclasificate, orice dosar închis trebuie să rămână închis, păstrând referinţa lor	D

Ref	Cerinţe	Testabil
	din schema de clasificare (codul de clasificare) anterior schimbării.	
3.4.11.	Dacă vreo clasă, volum, sub-dosar sau act sunt relocate sau reclasificate, orice dosar deschis va trebui: ▪ ori să fie închis, păstrând referinţa din schema de clasificare anterioară schimbării şi să primească în metadate o referinţă încrucişată către un nou dosar din schema modificată; ▪ ori să primească o referinţă în schema modificată, dar obligatoriu să reţină în metadate toate referinţele din schema de clasificare anterioară schimbării, conform deciziei rolului de administrator care desfăşoară repoziționarea.	D
3.4.12.	Atunci când clasele sunt repoziționate sau copiate, SMAE trebuie să activeze moștenirea opțională a metadatelor aparținând claselor și a conținutului acestora (sau a copiilor) din noile clase mamă. *Această cerință include elemente precum autorizații de acces și clasificări de securitate.*	D
3.4.13.	Dacă vreo clasă este repoziționată sau copiată, SMAE trebuie să poată aplica orice programare de păstrare şi dispoziţie ce poate fi moştenită, de la noua clasă-mamă către clasele repoziționate sau copiate şi către conţinutul lor, suplimentar faţă de programările de păstrare şi dispoziţie existente. *Aceasta este o minimă funcționalitate cerută; SMAE poate oferi alte posibilităţi suplimentare pentru a aborda regulile de păstrare şi dispoziţie.* *Această cerinţă poate cauza conflicte între reguli; dacă apar conflicte, acestea trebuie tratate asemănător cu specificațiile din secţiunea 5.1 (în special 5.1.8 și 5.1.33).*	D
3.4.14.	Atunci când orice clasă este repoziţionată sau copiată, SMAE trebuie să solicite unui rol de administrator să introducă motivația repoziţionării sau copierii în metadate. *Introducerea unui motiv este obligatorie, deoarece aceste repoziţionări sau copieri sunt excepţionale, fiind potenţial periculoase pentru integritatea actelor dacă nu sunt administrate cu atenţie.*	D
3.4.15.	Atunci când vreo clasă, dosar sau act sunt repoziţionate sau copiate, SMAE trebuie să înregistreze situația lor anterior repoziţionării sau copierii în evidenţa de auditare.	D
3.4.16.	Atunci când orice clasă este repoziţionată sau reclasificată, SMAE trebuie să înregistreze valorilor metadatelor lor anterioare repoziţionării.	D

Ref	Cerinţe	Testabil

Ambele cerinţe de mai sus sprijină nevoia de a putea stabili istoricul actelor ce au fost repoziţionate.

3.4.17. SMAE trebuie să permită unui rol de administrator să marcheze clasa sau dosarul ca inactiv, pentru a preveni adăugarea de noi dosare la clasă sau de acte la respectivul dosar. D

3.4.18. SMAE ar trebui să permită unui rol de administrator să şteargă o clasă goală. D

3.4.19. SMAE trebuie să împiedice ştergerea unui dosar electronic sau a oricărei părţi din conţinutul său în orice moment. D

Această cerință este supusă excepţiilor în cazul:

distrugerii, în conformitate cu programarea de păstrare şi dispoziţie , așa cum este explicat la 5.1.25.

sau

ştergerii de către un rol de administrator, ca parte a procesului de auditare — vezi secţiunea 9.3.

3.4.20. SMAE trebuie să permită unui dosar electronic să fie închis de către un rol de utilizator. D

Această cerinţă este diferită de cea din MoReq, care limita această funcţie la administratori.

3.4.21. Un SMAE ar trebui să permită închiderea unui volum al unui dosar electronic în mod automat la îndeplinirea criteriilor specificate, definite la configurare, care includ cel puţin: D

- volume delimitate printr-o dată-limită anuală; de exemplu, sfârşitul anului calendaristic, al anului financiar, sau a unui ciclu anual definit;
- perioada de timp de la un eveniment specificat; de exemplu, cea mai recentă adăugare a unui act electronic la volum;
- numărul de acte electronice conţinute în volum.

Alte criterii sunt de dorit, în situaţii speciale, de pildă atunci când mărimea volumului atinge capacitatea de stocare a discului.

3.4.22. Un SMAE trebuie să facă accesibil conţinutul claselor, dosarelor, sub-dosarelor şi volumelor închise la fel ca şi pentru dosarele deschise, fără a face nici o diferenţiere între „deschis” şi „închis”. D

Altfel spus, utilizatorii care caută sau parcurg informaţia folosind SMAE nu trebuie să fie avertizaţi că dosarul etc. este închis sau deschis; şi trebuie

Ref	Cerinţe	Testabil
	aplicate aceleaşi facilităţi de căutare şi reguli de acces.	
3.4.23.	SMAE ar trebui să permită utilizatorilor să creeze referinţe încrucişate (adică legături de tipul: „vezi şi”) între dosarele înrudite.	D
3.4.24.	SMAE ar trebui să aibă capacitatea de a crea multiple intrări pentru un act electronic în mai multe clase, dosare, sub-dosare şi volume electronice, fără duplicarea actelor sau a documentului pe care se bazează. *MoReq2 nu specifică cum trebuie realizată această cerinţă. O cale de a satisface această cerinţă ar fi să se folosească indicatori (*pointers*) la captura mai multor acte pe baza aceluiaşi document.*	D
3.4.25.	SMAE trebuie să furnizeze rolului de administrator instrumente de raportare cu scop statistic despre aspectele legate de activitatea din cadrul schemei de clasificare, incluzând numerul şi mărimea claselor, dosarelor, volumelor sub-dosarelor şi a actelor create, închise sau şterse într-o anumită perioadă. *Raportarea ar trebui să fie totală sau pe oricare utilizator sau clasă.*	D
3.4.26.	SMAE ar trebui să furnizeze capacităţi de raportare ad-hoc asupra aspectelor activităţii din cadrul schemei de clasificare.	P
3.4.27.	Orice utilizator care operează cu o clasă, dosar sau act trebuie să poată descoperi contextul acelei clase, dosar sau act, altfel spus metadatele şi clasa sau dosarul-mamă; şi trebuie să poată naviga către aceşti părinţi din clasă, dosar sau act. *Trebuie să fie posibil să se descopere contextul fără a fi nevoie să se părăsească clasa sau dosarul, de o manieră care să permită ca activitatea cu respectivul dosar să fie continuată fără întrerupere.*	D
3.4.28.	Ori de câte ori un cuvânt cheie al unui dosar este schimbat, SMAE trebuie să solicite unui rol de administrator să introducă un motiv pentru schimbare.	D
3.4.29.	Ori de câte ori un cuvânt cheie al unui dosar este schimbat, SMAE trebuie să solicite unui rol de administrator să introducă un motiv pentru schimbare. *Aceste monitorizări ale modificării cuvintelor cheie sunt cerute pentru a preîntâmpina riscul ca actele să fie ascunse prin schimbările de cuvinte cheie. Deoarece cuvintele cheie sunt folosite pentru a regăsi actele, este necesar să fie urmărite orice modificări produse asupra cuvintelor cheie pentru a evita posibilitatea ca un utilizator să încerce să ascundă un act prin modificarea cuvintelor sale cheie.*	D

4. Control şi securitate

Acest capitol aduce laolaltă cerinţe pentru o gamă largă de elemente de control referitoare la securitatea actelor. Aceste cerinţe furnizează caracteristici necesare pentru protecţia caracteristicilor actelor aşa cum sunt ele definite de ISO 15489 (secţiunea 7.2.).

Este esenţial pentru organizaţii să fie capabile de a controla cine are permisiunea de a accesa actele şi în ce situații, deoarece documentele pot conţine date personale, comerciale/economice sau secrete operaţionale.

Poate fi de asemenea necesar ca restricţiile asupra accesului să fie aplicate utilizatorilor externi. De pildă, în unele ţări în care legislaţia cu privire la libertatea de informare permite accesul la anumite acte publice, utilizatorii pot dori să vadă anumite acte. De asemenea, unele organizaţii pot dori să pună părţi ale propriului depozitului SMAE în comun cu organizaţiile partenere. Cerinţele pentru aceste elemente de control sunt listate în secţiunea 4.1.

Orice acces la acte şi la alte activităţi care le implică şi la documentaţia sau la date înrudite trebuie de asemenea să fie înregistrate în evidenţa de auditare, pentru a asigura admisibilitatea juridică şi pentru a ajuta la recuperarea datelor. Cerinţele pentru aceste controale ale evidenţei de auditare sunt listate în secţiunea 4.2; aceste cerinţe se adresează în principal caracteristicilor de autenticitate şi integritate ale actelor, așa cum sunt definite în ISO 15489 (secţiunea 7.2).

Securitatea actelor include de asemenea şi capacitatea de a le proteja de căderile de sistem prin intermediul copiilor de siguranță şi capacităţii de recuperare a actelor din copiile de siguranță. Aceste cerinţe sunt listate în secţiunea 4.3; aceste cerinţe sunt legate de caracteristica de utilizabilitate a actului, definită în ISO 15489 (secţiunea 7.2).

Actele vitale sunt actele esenţiale pentru misiunea organizaţiei şi trebuie să fie recuperate rapid după dezastru. Acestea sunt prezentate în secţiunea 4.4.

4.1 Acces

Organizaţiile trebuie să controleze accesul la actele lor şi aceasta se produce în mod obişnuit prin specificarea şi implementarea de politici de securitate, adică accesul la acte este acordat pe baza rolului pe care îl joacă în activitate o persoană din cadrul organizaţiei. Utilizatorii sunt de obicei administraţi centralizat şi drepturi de acces se acordă simultan pentru un număr de sisteme ale corporaţiei, incluzând, dar nu numai, pentru SMAE.

Nu este considerată bună practică administrarea permisiunilor dintr-un SMAE doar prin alocarea de permisiuni individuale anumitor utilizatori pentru entități specifice. Drepturile de acces vor fi prin urmare în mod normal acordate pentru roluri şi/sau grupuri, pentru a le permite acestora să salveze şi să opereze cu actele din anumite clase sau dosare din cadrul schemei de clasificare.

În plus faţă de acordarea accesului la anumite părţi din schema de clasificare, permisiunile restricţionează de asemenea acţiunile pe care un utilizator, rol sau grup le poate desfăşura asupra entităţilor din cadrul SMAE, cum ar fi inspectarea metadatelor şi a conţinutului lor şi modificarea sau ştergerea acestora, și crearea sau vizualizarea entităţilor de un anumit fel.

De exemplu, un rol de utilizator poate căuta şi citi acte, dar securitatea bazată pe roluri a organizaţiei poate restrânge capacităţile de căutarea şi de citire ale unor subseturi particulare ale schemei de clasificare.

Permisiunile pot fi acordate grupurilor şi pot fi moştenite de membrii grupului. Aplicarea permisiunilor la nivel de grup și nu la nivel de utilizator îmbunătăţeşte administrarea SMAE în timp, când noi utilizatori sosesc, şi utilizatorii existenţi se schimbă sau pleacă.

Prin atribuirea de roluri în SMAE, permisiuni multiple pot fi acordate automat unui utilizator şi unui grup. Mai târziu, atunci când utilizatorul sau grupul sunt scoase din rolul pe care l-au avut, toate permisiunile sunt automat scindate.

SMAE trebuie să fie capabil să limiteze setările acestor drepturi de acces la anumite roluri. În tabelul din 13.4, este indicat că această atribuție aparţine rolurilor de administrator.

Este de observat totuşi că rolurile de administrator doar implementează, din perspectiva sistemului, deciziile politice ale conducerii superioare. Politicile de securitate şi atribuirea lor utilizatorilor finali individuali se bazează în mod obişnuit pe nevoile din activitate ale utilizatorilor de a accesa informaţiile, politica organizaţiei asupra actelor şi legi şi regulamente, cum ar fi legi asupra libertății de informare, legi de protecţie a datelor personale, legi ale arhivelor şi regulamente ale industriei; la acestea se face referire în secţiunea 11.5.

În anumite medii, permisiunile de acces din SMAE sunt administrate integral din interiorul SMAE. În altele, anumite permisiuni sunt administrate folosind software-uri separate, cum ar fi utilităţile sistemului de operare al reţelei. Ambele sunt acceptabile pentru conformitatea cu următoarele cerinţe.

Rolurile identificate au doar un caracter de exemplificare. Ar trebui ca organizaţiile să stabilească numărul şi structura rolurilor pe care le utilizează sau dacă foloseşte vreun rol, în conformitate cu cerinţele proprii.

Ref	Cerinţe	Testabil
4.1.1.	SMAE trebuie să nu permită nici unei persoane să desfăşoare o activitate în cadrul unui SMAE decât dacă persoana este un utilizator autentificabil, care s-a identificat şi autentificat cu succes. *MoReq2 nu specifică natura mecanismului de autentificare. În multe situaţii, un nume de utilizator şi o parolă sunt considerate ca furnizând o autentificare suficientă. Organizaţiile care folosesc MoReq2 pentru scopuri de achiziții au nevoie să se asigure că un nivel corespunzător de autentificare este inclus.*	D
4.1.2.	Un SMAE trebuie să permită rolului de administrator să atribuie accesul la acte, sub-dosare, dosare, clase şi metadate unui rol de utilizator şi/sau grup de utilizatori specificat şi pentru anumite perioade de timp.	D

4.1.3. SMAE nu trebuie să introducă o limită a numărului de roluri care poate fi configurat. P

4.1.4. SMAE trebuie să permită unui rol de administrator să se asigure mentenanța permisiunilor pentru toate rolurile şi grupurile. Aceastea determină funcţionalităţile, elementele de metadate, actele sau dosarele la care rolurile şi grupurile au acces şi tipul de acces permis. D

4.1.5. SMAE trebuie să permită rolurilor de administrator să folosească permisiunile pentru a: P

- restricţiona accesul la anumite dosare sau acte;
- restricţiona accesul la anumite clase din schema de clasificare;
- restricţiona accesul în conformitate cu autorizațiile de securitate ale utilizatorilor (acolo unde este cazul);
- restricţiona accesul la anumite caracteristici şi funcţii (de exemplu, actualizare şi/sau ştergerea anumitor elemente de metadate);
- nega accesul după o anumită dată;
- permite accesul după o dată specificată.

Permisiunile ar trebui să fie folosite pentru a aloca accesul în conformitate cu politicile de securitate ale organizației

Nivelul de detaliere cerut este indicat în secțiunea 13.4

4.1.6. SMAE ar trebui să permită configurarea de activare a accesului prin intermediul unei logări la o reţea integrată. D

4.1.7. SMAE trebuie să permită rolurilor de administrator să adauge şi să înlăture utilizatorii în şi din roluri şi grupuri în orice moment. D

Se accepta ca rolurile de administrator să administreze grupurile prin intermediul unui software separat de administrare a directoarelor.

4.1.8. SMAE trebuie să permită alocarea către diferitele roluri de administratori a drepturilor de administrare asupra diferitelor secţiuni ale schemei de clasificare. D

Pentru exemplificare, vezi modelul de control al accesului din secţiunea 13.4.

4.1.9. SMAE trebuie să permită rolurilor de administrator să marcheze un utilizator individual ca inactiv, fără a şterge respectivul utilizator din sistem. D

Se accepta ca rolurile de administrator să administreze grupurile prin intermediul unui software separat de administrare a directoarelor.

4.1.10. SMAE trebuie să permită rolurilor de administrator să definească aceleaşi funcţii de control pentru rolurile de utilizator, cât şi pentru utilizatori.

Această caracteristică permite rolurilor de administratori să administreze şi să întreţină mai degrabă un set limitat de drepturi de acces al rolurilor decât un număr mare de utilizatori individuali. Exemple de roluri pot include manageri, funcționar privind rezolvarea reclamațiilor, analist de securitate, administrator de bază de date.

4.1.11. SMAE trebuie să fie capabil să aplice selecţii ale cerinţelor de acces care să nu fie limitate în cadrul unui rol. D

Pentru exemple vezi secţiunea 13.4.

4.1.12. SMAE trebuie să permită unui rol de administrator să seteze şi să întreţină grupurile de utilizator. D

Exemple de grupuri ar putea fi Resursele umane, Echipa de nord de vânzări.

4.1.13. SMAE trebuie să permită unui utilizator să fie membru al mai multor grupuri. D

Este posibil ca unii utilizatori să aibă cerinţe diferite de acces pentru diferite părţi ale schemei de clasificare. În toate cazurile, utilizatorii vor fi alocați unor grupuri de către rolurile de administrator, ca răspuns la nevoile şi politicile activităţii.

4.1.14. SMAE trebuie să permită rolului de administrator să seteze liste ad-hoc de utilizatori individuali, cu scopul de a controla accesul la anumite părţi ale schemei de clasificare sau acte. D

4.1.15. SMAE trebuie să rezerve funcţiile sistemului şi evenimentele asociate doar pentru rolurile de utilizatori. D

Această cerință este necesară pentru a păstra caracteristica de autoritate a actele electronice.

4.1.16. SMAE trebuie să permită doar rolului de administrator să seteze profiluri de utilizator şi să aloce utilizatorii către grupuri şi roluri. D

Vezi de asemenea şi secţiunea 13.4.

4.1.17. SMAE trebuie să permită rolurilor care răspund de anumite acte să specifice ce alţi utilizatori sau grupuri pot accesa respectivele acte. D

Vezi glosarul pentru semnificația în cadrul MoReq2 a termenului „responsabil”. Dacă politica organizaţională permite, responsabilitatea trebuie să aparţină rolului de administrator.

4.1.18. SMAE trebuie să restricţioneze capacitatea de a face schimbări, cum ar fi adăugarea, modificarea şi ştergerea profilurilor grupurilor, rolurilor sau utilizatorilor pentru rolurile de administrator. D

Aceasta include atribute cum ar fi drepturi de acces, autorizaţii, alocări şi administrare de parole.

4.1.19. SMAE trebuie să permită rolurilor administrative să seteze şi să administreze reguli pentru a gestiona accesul utilizatorilor la funcţiile SMAE, astfel încât diferitele roluri să aibă acces la diferitele combinaţii de funcţii. SMAE trebuie să permită ca asemenea reguli să fie setate la cel mai mic nivel de detaliere (adică mărimea diviziunii) arătată în tabela ilustrată de drepturi de acces din secţiunea 13.4. D

Diverse organizaţii au diverse cerinţe funcţionale de control al accesului. Nu este prin urmare potrivită o încercare de a defini un model generic. Ca urmare, această cerinţă specifică în schimb nivelul de detaliu al controlului pe care un SMAE trebuie să îl ofere.

4.1.20. SMAE trebuie să permită rolurilor de administrator să creeze roluri adiţionale pentru cele arătate în 13.4. D

O organizaţie poate defini roluri cu drepturi de acces specifice, cum ar fi: lucrător de caz, manager etc.

4.1.21. SMAE ar trebui să furnizeze o interfață de programare a aplicației (API) pentru a furniza acces la acte prin inițierea acțiunii din altă aplicație sistem. N

4.1.22. Dacă un utilizator desfășoară o căutare de conţinut (în mod obişnuit, dar nu necesar, o căutare integrală sau liberă a textului), SMAE nu trebuie să includă în lista de rezultate nici un act pentru care utilizatorul nu are permisiunea de a vedea conţinutul.

Această cerinţă este necesară pentru a împiedica utilizatorii să folosească căutarea de text pentru a cerceta conţinutul documentelor la care nu le este permis accesul.

4.1.23. Dacă un utilizator solicită accesul, navigarea sau căutarea, fără a căuta conţinutul, oricărui obiect, cum ar fi act, volum, sub-dosar, dosar sau clasă la care utilizatorul nu are permisiune de acces, SMAE trebuie să furnizeze unul din următoarele răspunsuri (răspunsurile trebuie selectate la data configurării): D

- să nu furnizeze nici o informaţie despre obiect, astfel ne-furnizând nici o indicaţie dacă obiectul există sau nu,
- confirmă existenţa şi (opţional) deţinătorul obiectului (afişează dosarul sau identificatorul actului), dar nu titlul său sau alte metadate;

- afişează titlul, genul entităţii (clasă, act etc.), data creării şi a deţinătorului;
- afişează titlul şi alte metadate ale obiectului.

Opţiunea de la prima bulină a acestei cerinţe specifică acelaşi rezultat ca şi pentru căutarea în conţinut (vezi 4.1.22). Celelalte 3 opţiuni oferă intenţionat alte posibilităţi, potrivite pentru unele organizaţii; acestea sunt prezentate aici în ordinea inversă a securităţii. Acestea ar trebui să fie configurate de rolurile de administrator.

Aceste cerinţe se aplică doar încercărilor de acces care nu implică căutarea conţinutului unui act. Căutările în conţinutul actului sunt tratate în 4.1.22, împreună cu care această cerinţă ar trebui citită.

4.1.24. SMAE ar trebui să permită ca răspunsurile specificate în 4.1.23 să fie selectate pentru o clasă ca o alternativă la configurarea generală a sistemului, în momentul configurării sau mai târziu. D

4.2. Evidenţa de auditare

O evidenţă de auditare este o mărturie a acţiunilor desfăşurate care implică SMAE. Aceasta include acţiunile desfăşurate de către rolurile de administratori sau de utilizatori sau acţiuni iniţiate automat de către SMAE ca efect al unor parametrii de sistem. Vezi glosarul de la secţiunea 13.1 pentru o definiţie oficială.

Evidenţa de auditare indică în ce măsură regulile de activitate au fost urmate şi asigură că activitatea neautorizată poate fi identificată şi urmărită.

Pentru a sprijini răspunderea, este esenţial ca SMAE să fie capabil să înregistreze în evidenţa de auditare orice acţiune în care orice grad de prelucrare automată sau asistată de calculator este implementată în interiorul sistemului. Secţiunea 10.5 *Activitatea de caz* furnizează exemple pentru o astfel de interfaţă.

Evidenţa de auditare este un factor esenţial pentru a permite SMAE să îndeplinească aceste cerinţe prin păstrarea unor înregistrări complete a tuturor acţiunilor desfăşurate asupra fiecărui act (supuse constrângerilor la nivel de securitate a mediului tehnic).

Volumul informaţiilor din evidenţa de auditare poate deveni foarte mare dacă toate acţiunile sunt auditate. Ca urmare, în unele implementări, conducerea poate decide dacă acţiunile selectate trebuie să nu fie incluse în evidenţa de auditare (după data deciziei).

În multe implementări, evidenţa de auditare online este transferată periodic în depozite offline exemplarul offline fiind supus ştergerii dacă şi când actele relevante sunt şi ele selecţionate; sau dacă şi când politicile şi legislaţia permit.

Acestea sunt subiecte de politica administrativă şi/sau cerinţe legale şi de reglementare. MoReq2 prin urmare include cerinţe de sistem care să permită asemenea acţiuni, dar nu stabileşte în ce măsură acestea sunt folosite.

Ref	Cerință	Testabil
4.2.1.	SMAE trebuie să păstreze o evidenţă de auditare nechimbată, capabilă să captureze şi să stocheze informaţii despre: ▪ orice acţiune desfăşurată asupra oricărui act, grupare sau schemă declasificare; ▪ utilizatorul care a desfăşurat acţiunea; ▪ data şi ora acţiunii. *Pentru exemplificare, acţiunile înregistrate de evidenţa de auditare trebuie să includă, dar nu trebuie să se limiteze la:* ▪ *captura tuturor actelor electronice;* ▪ *reclasificarea oricărui act electronic în cadrul schemei (vezi 3.4.1);* ▪ *orice schimbare asupra oricărei programări de păstrare şi dispoziţie;* ▪ *orice acţiune de revizuire a dispoziţiei desfăşurată de rolurile de administrator;* ▪ *aplicarea sau anularea unei suspendări de dispoziţie asupra unui dosar electronic;* ▪ *orice modificare producă oricărei metadate asociate cu clasele, dosarele electronice sau actele electronice;* ▪ *amendarea sau ştergerea metadatelor de către un utilizator;* ▪ *schimbările făcute pentru permisiunile de acces;* ▪ *crearea, amendarea sau ştergerea unui utilizator sau unui grup;* ▪ *exportul sau transferul;* ▪ *crearea unei prezentări;* ▪ *ştergerea/distrugerea actelor*. *Termenul ,,neschimbată" din această cerinţă înseamnă că trebuie să fie imposibil pentru orice utilizator să schimbe sau să şteargă orice parte a evidenţei de auditare. Nivelul de asigurare care poate fi atins va depinde de nivelul de securitate al sistemului de operare de bază şi de aplicaţia de sistem.* *Evidenţa de auditare poate fi, totuşi, supusă re-organizării şi/sau copierii într-o stocare offline dacă este cerut, de pildă, de un software de baze de date, atât timp cât integritatea sa rămâne intactă.*	D
4.2.2.	Acolo unde SMAE acceptă transferul datelor din evidenţa de auditare către o stocare offline, SMAE trebuie să accepte procese securizate pentru administrarea datelor offline şi să demonstreze cum datele offline pot fi readuse la momentul şi în maniera solicitată; şi SMAE trebuie să se asigure că	P

nu este posibil ca acest mecanism să fie folosit ca un mijloc de a ocoli controalele impuse de SMAE (de exemplu, prin simpla mutare a datelor din evidenţa de auditare în afara SMAE şi modificarea sau ştergerea acesteia în exteriorul sistemului).

4.2.3. SMAE ar trebui să poată înregistra automat în evidenţa de auditare orice accesare a vreunui act sau grupări şi dacă accesul a fost făcut pentru a citi, tipări sau pentru o altă formă de prezentare. D

Această cerinţă este necesară, în mod normal, doar în mediile cu securitate sporită.

4.2.4. Parametrii evidenţei de auditare a SMAE trebuie să fie astfel configuraţi încât rolurile de administrator să poată configura ce acţiuni sunt înregistrate automat. D

4.2.5. Toate schimbările parametrilor din evidenţa de auditare trebuie la rândul lor să fie înregistrate în evidenţa de auditare. D

Nu trebuie să fie posibil niciodată ca auditarea schimbărilor din evidenţa de auditare să fie întreruptă, astfel încât SMAE să nu se înregistreze în evidenţa de auditare cine a realizat modificarea şi când.

4.2.6. Odată ce parametrii evidenţei de auditare au fost setaţi, SMAE trebuie să înregistreze automat acţiunile şi trebuie să stocheze informaţia despre ele în evidenţa de auditare. D

4.2.7. SMAE trebuie să menţină evidenţa de auditare pentru atât timp cât este considerat necesar prin politica organizaţiei de păstrare a documentelor. N

Aceasta va fi adesea cel puţin durata de viaţă a actelor la care se referă evidenţa de auditare. Totuşi, pot exista situaţii în care alte politici se aplică, de pildă controlul periodic al evidenţei de auditare, urmat de distrugerea şi înlocuirea printr-un certificat de control.

4.2.8. SMAE trebuie să înregistreze în evidenţa de auditare toate acţiunile desfăşurate asupra actelor, volumelor, sub-dosarelor, dosarelor, claselor şi termenelor de păstrare şi dispoziţie, indiferent dacă acţiunea a afectat una sau mai multe dintre ele. D

4.2.9. SMAE trebuie să înscrie în evidenţa de auditare toate schimbările valorilor de metadate care se aplică elementelor listate în modelul de metadate MoReq2.

4.2.10. Orice adnotare sau modificare adusă unui act trebuie să fie înregistrată în evidenţa de auditare a actului. D

4.2.11. SMAE trebuie în mod automat să înscrie în evidenţa de auditare toate schimbările aduse parametrilor administrativi. D

De pildă, dacă un rol de administrator schimbă permisiunile de acces sau reconfigurarea evidenţei de auditare.

4.2.12. SMAE trebuie să se asigure ca datele din evidenţa de auditare să fie disponibile pentru inspecţie la cerere, astfel încât un anumit eveniment să poată fi identificat şi toate datele înrudite să fie făcute accesibile. D

4.2.13. SMAE trebuie să includă caracteristici care să permită tuturor utilizatorilor autorizaţi, chiar și cei care sunt puțin sau deloc familiarizaţi cu sistemul, să caute informaţiile în evidenţa de auditare. P

Aceasta este o cerinţă pentru uşurinţă în folosire. Aceşti utilizatori pot fi externi organizaţiei, cum ar fi auditorii externi. Cu toate acestea, din perspectiva SMAE, ei vor fi utilizatori.

4.2.14. SMAE trebuie să permită utilizatorilor să caute în evidenţa de auditare anumite evenimente, obiecte (clase, acte etc.), utilizatori, grupuri, roluri, momente sau intervale de timp. D

4.2.15. SMAE trebuie să fie capabil să exporte datele din evidenţa de auditare pentru anumite acte, volume, sub-dosare, dosare şi clase fără afectarea evidenţa de auditare stocată de SMAE. D

Această funcţionalitate trebuie să permită, de exemplu, auditorilor externi, să examineze sau să analizeze activitatea sistemului.

4.2.16. SMAE trebuie să poată permite captura şi stocarea, acolo unde este cazul, a oricăror tentative de violare a mecanismelor de control a accesului (de pildă, o încercare a unui utilizator de a accesa un act, volum, sub-dosar sau dosar la care nu i se permite accesul). D

Pentru o ilustrare a circumstanţelor care pot permite tentative de violare, vezi 4.1.23. Aceasta nu se poate aplica atunci când sistemul este configurat să ascundă unui utilizator orice cunoaștere a informaţiei pentru care acestea nu are autorizaţie de acces.

4.3. Copierea de siguranță şi recuperarea

Cerinţele de reglementare şi de activitate solicită ca unui SMAE să îi fie furnizate comenzi cuprinzătoare pentru a furniza copii de siguranță periodice ale actele şi metadatelor; şi să fie capabil de a recupera rapid actele dacă unul dintre ele este pierdut din cauza unei căderi de sistem, accident, breșă de securitate etc.

Copiile de siguranță şi recuperările automate periodice pot fi furnizate de SMAE sau prin integrarea cu servicii sau utilităţile unui Sistem de Management al Documentelor Electronice (EDMS/SMDE), printr-un sistem de administrare a bazei de date operând cu SMAE sau prin alt software. În această secţiune, menționarea ca „SMAE” poate însemna oricare din aceste cazuri, potrivit setărilor.

În practică, funcţiile de copiere de siguranţă şi de recuperare pot fi mai mult în sarcina zonei de operaţii IT din organizaţie decât să fie împărţite între rolurile de administrator ale SMAE.

Ref	Cerinţe	Testabil
4.3.1.	SMAE trebuie sa furnizeze sau să permită proceduri automate de copiere de siguranță şi recuperare care să permită copierea de siguranță periodică a tuturor claselor, dosarelor, actelor, metadatelor, parametrilor administrativi sau a evidenţei de auditare a unui SMAE sau doar a celor selectate, precum şi recuperarea lor atunci când este necesar.	D
4.3.2.	SMAE trebuie să permită rolurilor de administrator să programeze capacitatea de a efectua copia de siguranță prin: ▪ specificarea frecvenţei copierii de siguranță; ▪ selectarea claselor, dosarelor şi actelor pentru care trebuie copiate de siguranță; ▪ alocarea de medii de stocare, sisteme sau destinaţii pentru copiile de siguranță (de pildă, stocarea offline, sisteme separate, site-uri la distanţă).	D
4.3.3.	SMAE trebuie să permită doar rolurilor de administratori autorizaţi să refacă starea unui SMAE din copiile de siguranță.	D
4.3.4.	Atunci când SMAE este refăcut dintr-o copie de siguranță, integritatea completă a datelor incluse în evidenţa de auditare trebuie să fie menţinută după refacere. *Actele care au fost corect eliminate şi care sunt prezente în copia de siguranţă nu ar trebui să fie refăcute decât în cazuri excepţionale.*	P
4.3.5.	Acolo unde SMAE prezintă puncte de control şi capacități de *roll-forward* ale bazei de date, SMAE trebuie să permită doar rolurilor de administratori să efectueze *roll-forward*.	P

4.4 Acte vitale

Actele vitale sunt acele acte care sunt considerate absolut esenţiale pentru capacitatea organizaţiei de a-şi îndeplini funcţiile activităţii, pe termen scurt, pe termen lung, sau amândouă (vezi de asemenea şi glosarul). Acestea pot fi ori acte critice pentru misiunea instituțională în termeni de capacitatea de a se ocupa de situațiile de urgenţă/dezastru ori acte necesare pentru a proteja interesele pe termen lung de natură financiară şi juridică.

Identificarea şi protecţia unor astfel de acte este de mare importanţă pentru orice organizaţie şi este posibil să fie nevoie ca aceste acte să fie primele recuperate în caz de dezastru.

Actele pot fi considerate ca acte vitale fie pentru organizaţie ca întreg, fie pentru părţi ale organizaţiei.

Ref	Cerinţe	Testabil
4.4.1.	SMAE trebuie să permită rolurilor de administrator să indice dacă dosarele sau actele selectate conţin sau sunt considerate a fi acte vitale. *Această indicaţie ar trebui inclusă ca element de metadate.*	D
4.4.2.	SMAE trebuie să furnizeze două operaţiuni distincte pentru copierea de siguranță. ▪ copie de siguranță „integrală”, care se bazează pe salvarea tuturor datelor (specificate) din SMAE ▪ copie de siguranță „vitală”, care salvează doar configuraţia SMAE şi dosarele şi actele identificate ca „vitale”. *Sunt folosite două operaţiuni pentru copierea de siguranță pentru a permite:* ▪ *să fie programate copii de siguranță vitale mai frecvent decât copii de siguranță integrale ale SMAE.* ▪ *să fie încărcate copiile de siguranță vitale pe suporturi diferite şi stocate separat de (şi posibil`, mai securizat decât) copiile de siguranță integrale*. *Se oferă de asemenea, o mai bună administrare a refacerii SAME, atunci când refacerea din copii de siguranță vitale se poate produce integral, independent de şi la un moment diferit de refacerea completă.* *Aşa cum este specificat în secţiunea 4.3, copia de siguranță poate fi realizată atât de către un SAME, cât şi de un alt software integrat.*	D
4.4.3.	După recuperarea dintr-o copie de siguranță „vitală”, SMAE trebuie să fie complet operaţional. *După refacerea dintr-o copie de siguranță „vitală”, multe dosare şi acte nu vor fi prezente. Cu excepția acestei situații, totuşi, SMAE nu trebuie să fie în nici un fel limitat în operarea sa sau în funcţionalitatea pe care o oferă utilizatorilor.*	P
4.4.4.	SMAE trebuie să furnizeze două metode de refacere din copia de siguranță completă: ▪ restabilire într-un mediu „curat”, în care datele din copia de siguranță completă rescriu şi înlocuiesc SMAE în timpul operaţiunii de recuperare; ▪ restabilire peste un mediu existent, în care datele din copia de siguranță „completă” sunt reintegrate într-un mediu SMAE	D

existent.

Prima metodă de refacere va fi comună în organizaţiile unde copiile de siguranță vitale nu sunt realizate. A doua metodă de refacere se va aplica atunci când un SMAE a fost parţial refăcut înainte dintr-o copie de siguranță vitală şi s-a reîntors la operarea normală; devine atunci necesar să fie integrată copia de siguranță completă, fără suprascrierea fie a actelor şi dosarelor vitale care au fost anterior refăcute, fie a noilor entităţi care au fost adăugate, fie a schimbărilor care s-au produs în SMAE, în intervalul de când s-a întors la operare completă.

Dacă SMAE acceptă două metode de refacere dintr-o copie de siguranță completă, aşa cum este schiţat în 4.4.4, copia de siguranță vitală (dacă există) va fi întotdeauna refăcută prima. Nu este necesar să se ia în considerare refacerea dintr-o copie vitală de siguranță peste o copie integrală de siguranță.

Când se desfăşoară o revenire de sistem din două părţi în acest fel, poate fi necesar ca rolurile de administrator să rezolve manual orice conflict care apare. De exemplu, schema de clasificare poate fi afectată într-o copie de siguranță față de alta.

4.4.5. SMAE trebuie să permită rolurilor de administrator să indice acele acte care nu mai sunt vitale. Această acţiune trebuie înregistrată în evidenţa de auditare. D

De exemplu, un contract sau o înţelegere de închiriere poate expira şi prin urmare nu va mai fi considerat vital.

5. Păstrarea şi dispoziţia

Acest capitol prezintă cerinţe pentru folosirea promgramărilor de păstrare şi dispoziţie care să guverneze păstrarea şi soarta ulterioară a actelor rezultate din operaţiunile în desfăşurare. Programările de păstrare şi dispoziţie stabilesc pentru cât timp actele trebuie păstrate de către SMAE şi cum trebuie eliminate. Cerinţele pentru programările de păstrare şi dispoziţie sunt listate în secţiunea 5.1; o definiţie oficială există în glosar.

Procesele care pot avea loc la data specificată de programările de păstrare şi dispoziţie sunt descrise în secţiunile următoare. Cerinţele pentru procesele de revizuire sunt listate în secțiunea 5.2 şi cerinţele pentru transfer, export şi distrugere sunt prezentate în secţiunea 5.3.

După cum este explicat în secţiunea 2.2, sub titlul *Dosare electronice, sub-dosare şi volume*, actele pot fi administrate în clase, dosare, sub-dosare şi volume, conform cerinţelor de activitate. În funcţie de situaţie, programările de păstrare şi dispoziţie se aplică claselor, dosarelor şi/sau sub-dosarelor şi/sau volumelor. Programările de păstrare şi dispoziţie pot de asemenea să fie aplicate genurilor de acte, de pildă, să se aplice termene de păstrare pentru datele personale confidenţiale sau termene de păstrare lungi planurilor inginereşti. Rezolvarea conflictelor între programările de păstrare şi dispoziţie sunt de asemenea permise.

MoReq2 include conceptul de ,,suspendare de dispoziţie", care nu a existat în versiunea anterioară a MoReq. Suspendările de dispoziţie sunt folosite ca răspuns la evenimente neaşteptate, pentru a asigura că actele specificate nu sunt distruse. Cel mai obişnuit exemplu este să se asigure că actele care sunt, sau care pot fi, cerute ca probă în procedurile juridice nu sunt distruse în mod obişnuit, ca rezultat al unei decizii de dispoziţie.

5.1. Programări de păstrare și dispoziție

Ref	Cerinţe	Test
5.1.1.	SMAE trebuie să permit rolurilor de administrator, şi doar acestora, să creeze şi să întreţină programări de păstrare şi dispoziţie	D
5.1.2.	SMAE nu trebuie să limiteze numărul programărilor de păstrare şi dispoziţie ,	P
5.1.3.	SMAE ar trebui să poată ordona programările de păstrare şi dispoziţie într-o structură ierarhică, similară cu programările de păstrare şi dispoziţie generale şi specifice ale organizaţiei, aprobate de autoritatea competentă. *O structură ierarhică uşurează administrarea a mai multor programări de păstrare și dispoziție.*	N

Ref	Cerinţe	Test
5.1.4.	SMAE trebuie să aloce un identificator unic pentru fiecare programare de păstrare și dispoziție, atunci când a fost creată.	D
5.1.5.	SMAE trebuie să permită ca un singur titlu să fie introdus pentru fiecare programare de păstrare şi dispoziţie , atunci când este creată.	D
5.1.6.	SMAE trebuie să păstreze un istoric ce nu poate fi modificat al schimbărilor şi ştergerilor (evidenţa de auditare) care sunt făcute asupra programărilor de păstrare şi dispoziţie , incluzând data schimbării sau ştergerii şi utilizatorul care a efectuat schimbările.	D
5.1.7.	SMAE trebuie să se asigure că orice amendament adus unei programări de păstrare şi dispoziţie este imediat aplicat tuturor entităţilor la care este aplicată programarea de păstrare şi dispoziţie .	D
5.1.8.	SMAE trebuie să ceară rolului de administrator care modifică sau şterge o programare de păstrare şi dispoziţie să introducă o motivaţie şi să stocheze această motivaţie în evidenţa de auditare. *Schimbările şi ştergerile de programări de păstrare şi dispoziţie trebuie să fie controlate cu atenţie, pentru a reduce riscurile unor distrugeri neautorizate de acte.*	D
5.1.9.	SMAE trebuie să fie capabil să importe sau să exporte programări de păstrare şi dispoziţie .	P
5.1.10.	SMAE trebuie să se asigure că fiecare clasă, dosar, sub-dosar şi volum are cel puţin o programare de păstrare şi dispoziţie . *Această cerinţă este inclusă pentru a se asigura că nici o entitate nu este creată fără o programare de păstrare şi dispoziţie şi să îmbunătăţească utilizarea.*	D
5.1.11.	Programarea de păstrare şi dispoziţie aplicată implicit pentru fiecare nouă clasă, dosar, sub-dosar sau volum ar trebui să fie moștenită de la structura superioară de care aparține (structura mamă). *Acolo unde acest lucru nu este posibil (pentru clasele de la cel mai înalt nivel al schemei de clasificare şi dacă nu se aplică nici o programare de păstrare şi dispoziţie preluată — vezi 5.1.18), ar trebui să se poată aplica o programare de păstrare şi dispoziţie predefinită.*	D
5.1.12.	Toate actele stocate direct într-o clasă trebuie să aibă întotdeauna atribuită o programare de păstrare şi dispoziţie .	D
5.1.13.	Programările de păstrare şi dispoziţie care se aplică implicit pentru orice nou act stocat direct într-o clasă (vezi secţiunea 3.2, 3.2.17) trebuie să fie preluate	D

Ref	Cerinţe	Test
	de la clasa mamă.	
5.1.14.	SMAE trebuie să permită unui rol de administrator să aplice o programare de păstrare şi dispoziţie pentru orice clasă, dosar, sub-dosar, volum sau gen de act, în orice moment. *Sintagma „în orice moment" înseamnă că rolul de administrator poate înlocui o programare de păstrare şi dispoziţie sau (dacă sistemul suportă mai multe programări de păstrare şi dispoziţie , vezi 5.1.16) aplica aplica o programare de păstrare şi dispoziţie adiţională, pentru orice clasă, dosar, sub-dosar volum sau gen de act. Un exemplu ar fi înlocuirea unei programări de păstrare şi dispoziţie implicite; un altul este aplicarea unei programări de păstrare şi dispoziţie adiţionale, ca răspuns la o investigaţie oficială. Aceasta poate determina un conflict între termenele de păstrare: vezi 5.1.23.*	D
5.1.15.	SMAE trebuie să poată aplica o programare de păstrare şi dispoziţie predefinită pentru genuri de documente. *Aceasta cerință implică faptul că un gen de act poate exista fără a avea aplicat nici o programare de păstrare şi dispoziţie . Acest lucru poate fi acceptat, deoarece fiecare act individual are cel puţin o programare de păstrare şi dispoziţie aplicată lui, deoarece fiecare acte este ţinut într-un dosar şi cerinţa 5.1.10 obligă ca cel puţin o programare de păstrare şi dispoziţie să fie aplicată fiecărui dosar.*	D
5.1.16.	SMAE trebuie să permită mai mult de un termen de păstrare să fie în vigoare pentru orice clasă, dosar, sub-dosar sau volum. *Aceasta cerință este cerută pentru a administra nişte scenarii reale, care implică cerinţe de păstrare ce rezultă din nevoi legale şi practice. Acestea sunt ilustrate de un exemplu, ales din mai multe posibile.* *În acest exemplu, dosarul are o singură o programare de păstrare şi dispoziţie , atribuită din raţiunile activității, în timp ce actele din cadrul dosarului nu se preconizează să fie subiect al cerinţelor juridice sau de reglementare. Programarea de păstrare şi dispoziţie aplicată acestui dosar se aplică de asemenea şi altor dosare. La un moment dat, se întrevede că ar putea fi nevoie ca acel dosar să fie păstrat pentru o perioadă de timp mai lungă decât prevede actuala regulă, datorită unui aspect al activităţii referitor la reglementări în domeniul siguranței. În acest moment, este probabil ca actele din conţinutul dosarului să poată deveni subiect al unui control de respectare a reglementărilor, cu referitor la regulile de siguranţă; deci o a doua programare de păstrare şi dispoziţie se aplică dosarului, luând noile realităţi în considerare. Ulterior, se poate observa faptul că problema de siguranţă nu există; în acest caz, o a doua programare de păstrare şi dispoziţie poate fi eliminată, lăsând în loc şi activă pe cea originală.*	D

Ref	Cerinţe	Test
5.1.17.	Păstrarea sau dispoziția oricărui act trebuie să fie guvernate de programarea (programările) de păstrare și dispoziție asociate cu clasa, dosarul, sub-dosarul, volumul şi categoria de care aparține actul respectiv; şi de către orice suspendare a dispoziției aplicabilă (vezi 5.1.34). *Odată ce o programare de păstrare şi dispoziţie este aplicată, aceasta guvernează păstrarea şi dispoziția actelor asociate cu entitatea căreia îi este aplicată (dacă nu este supra-guvernată de o programare de păstrare şi dispoziţie diferită).*	D
5.1.18.	SMAE trebuie să permită oricărei programări de păstrare şi dispoziţie să fie moștenită într-o schemă de clasificare, la opţiunea rolului de administrator. *Un rol de administrator poate selecta dacă o programare de păstrare şi dispoziţie este moştenită sau nu, folosind mijloacele corespunzătoare. MoReq2 nu precizează cum se produce acest lucru. Posibilităţile includ:* ▪ *opţiunea este selectată atunci când programarea de păstrare şi dispoziţie este creată (caz în care se aplică ori de câte ori programarea de păstrare şi dispoziţie este aplicată);* ▪ *ori de câte ori programarea de păstrare şi dispoziţie este aplicată (în care caz, se aplică tuturor entităților fiică);* ▪ *opţiunea este selectată atunci când o entitate este creată pentru a moşteni programarea de păstrare şi dispoziţie a entității mamă.*	D
5.1.19.	Fiecare programare de păstrare şi dispoziţie trebuie să includă: ▪ fie un termen de păstrare (5.1.25) şi un eveniment declanşator ▪ fie o dată de dispoziţie	D
5.1.20.	Fiecare programare de păstrare şi dispoziţie trebuie să includă: ▪ o acţiune de dispoziţie (5.1.24) ▪ o motivație	D
5.1.21.	Fiecare termen de păstrare ar trebui să includă: ▪ descriere ▪ o bază juridică *Bază juridică specifică justificarea pentru termenul de păstrare. Acesta este adesea o referinţă la lege, regulament sau la politica corporaţiei.*	D
5.1.22.	Atunci când termenul de păstrare aplicabil unui act datorită unei programări de păstrare şi dispoziţie ajunge la sfârşit, SMAE trebuie în mod automat să iniţieze procesul de decizie de dispoziție.	D

Ref	Cerinţe	Test

Aceasta poate însemna fie ca decizia este executată (supusă 5.2.4) sau poate însemna că acţiunea este cerută de către un rol de administrator (vezi 5.1.23). Unele organizații pot prefera să implementeze cea de-a doua opțiune, datorită riscului implicat de executarea automată.

5.1.23. Atunci când SMAE iniţiază o decizie de dispoziţie (conform cu 5.1.22), dacă se aplică alte programări de păstrare şi dispoziţie , cu diferite termene de păstrare şi/sau decizii de dispoziţie, atunci apare un conflict. Trebuie să fie posibil ca SMAE să fie astfel configurat încât să informeze automat rolul de administrator dacă un astfel de conflict apare, lăsând rolului de administrator să rezolve acest conflict. D

Cuvintele „trebuie să fie posibil" sunt incluse, pentru că nu se cere ca rolurile de administrator să intervină în toate situaţiile. Se acceptă ca SMAE să rezolve un conflict de o manieră automată; dar trebuie să fie posibil să fie configurat SMAE pentru a solicita intervenţia administrativă în cazul unui conflict.

Un conflict poate apărea deoarece:

- *unele programări de păstrare şi dispoziţie indică faptul că dispoziţia trebuie să fie iniţiată, în timp ce altele indică contrariul;*
- *diferite programări de păstrare şi dispoziţie indică decizii de dispoziţie diferite.*

În majoritatea cazurilor va fi simplu de stabilit care regulă prevalează.

Aceste conflicte se pot ivi în două situații:

- *toate programările conflictuale se aplică totalității unei grupări (cum ar fi un dosar);*
- *programările se aplică atât unei grupări, cât și unor acte din cadrul acestora (deoarece cea de-a doua se aplică anumitor genuri de acte care există în cadrul grupării*).

Dacă decizia rolului de administrare implică păstrarea actelor, hotărârea va trebui să includă schimbarea listei cu termene de păstrare şi dispoziţii care se aplică actelor, pentru a se asigura că nu există nici un conflict la momentul acestei acţiuni.

Intervenţia administrativă poate fi cerută atunci când nu pot fi definite în mod practic reguli care să rezolve corect aceste conflicte. De exemplu:

- *două programări de păstrare şi dispoziţie , derivând din obligaţii juridice diferite, pot specifica termene de păstrare diferite. În mod normal, decizia va fi de a păstra actele până la sfârşitul celei mai îndelungate dintre cele două perioade.*
- *o programare de păstrare şi dispoziţie poate specifica data de la*

Ref	Cerinţe	Test

care anumite acte pot fi înlăturate (în mod obişnuit, datorită prevederilor legislaţiei de protecţie a datelor personale). Dacă această dată este mai veche decât termenul de păstrare cu care intră în conflict dintr-o programare de păstrare şi dispoziţie , atunci decizia va depinde de ponderea relativă a celor două obligaţii.

Aceste situaţii se pot ivi atunci când un document aparţine unui gen de acte care permite aplicarea şi moştenirea unei reguli de dispoziţie de către acel act mai degrabă de la genul de acte decât de la gruparea în care este conţinut.

Decizia rolului de administrator poate include oricare variantă din următoarele:

- *înlăturarea uneia sau mai multor reguli conflictuale aplicate grupării sau actelor afectate;*
- *schimbarea uneia sau mai multor reguli conflictuale pentru a elimina conflictul;*
- *eliminarea tuturor regulilor conflictuale şi aplicarea uneia noi;*
- *folosirea opţiunii de ştergere excepţională specificată în secţiunea 9.3*

Toate aceste acţiuni, dacă nu sunt controlate cu atenţie, pot ridica semne de întrebare privind buna guvernare a actelor. Prin urmare, oricare dintre aceste acţiuni — modificarea programărilor de păstrare şi dispoziţie sau ştergerea actelor— trebuie să fie supusă unor proceduri scrise. În anumite situații, mai multe soluții de management, cum ar fi diviziunea muncii, vor fi mai potrivite.

Dacă decizia duce la rămânerea unor acte în grupare, care în mod normal nu ar fi fost păstrate, organizaţia ar putea de asemenea să aibă linii directoare pentru stocarea lor. Aceasta ar putea include păstrarea grupării la locul ei sau repoziționarea (vezi secţiunea 3.4) actelor rămase.

5.1.24. SMAE trebuie să permită cel puţin următoarele acţiuni de dispoziţie (aşa cum sunt definite în 5.1.20) pentru fiecare programare de păstrare şi dispoziţie : D

- păstrare permanentă
- prezentare pentru revizuire
- distrugere automată
- distrugere după primirea autorizației din partea unui rol de administrator
- transfer la o Arhivă sau în alt depozit (vezi glosarul)

Există un risc asociat cu implementarea opțiunii de „distrugere automată”, care este conturat în cerința anterioară; organizațiile vor trebui să echilibreze

Ref	Cerinţe	Test
	aceste riscuri versus beneficiile acțiunii automate.	
5.1.25.	SMAE trebuie să permită cel puţin următoarea combinaţie de evenimente declanşatoare şi de termene de păstrare: ▪ durata unei anumite perioade de timp după care clasa, dosarul, sub-dosarul sau volumul sunt deschise; ▪ durata unei anumite perioade de timp după care clasa, dosarul, sub-dosarul sau volumul sunt închise; ▪ intervalul unei anumite perioade de timp de când cel mai recent act a fost clasat într-o clasă, dosar, sub-dosar sau volum; ▪ intervalul unei anumite perioade de timp de când un act a fost retras dintr-o clasă, dosar, sub-dosar sau volum; ▪ intervalul unei anumite perioade de timp după un anumit eveniment extern (care eveniment este descris în listă şi va fi mai degrabă notificat SMAE de către administrator decât va fi detectat automat de către SMAE) (de exemplu, „după semnarea contractului” sau „…100 de ani după data naşterii”); ▪ „permanent”, indicând păstrarea pe termen lung a actului. *În timp ce precizarea de mai sus include aspecte generale, este posibil ca unele organizaţii să dorească să impună evenimente declanșatoare suplimentare şi/sau termene de păstrare suplimentare.* *Orice număr de evenimente externe poate fi legat de diferite reguli de reţinere şi dispoziţie.*	D
5.1.26.	SMAE nu trebuie sa limiteze durata termenului de păstrare.	P
5.1.27.	SMAE trebuie să accepte termene de păstrare până la cel puţin 100 de ani pentru cerinţa 5.1.24. *Acest maxim este sugerat ca o perioadă arbitrară menită să evite orice limitare practică. Deşi este improbabil ca un SMAE să existe 100 de ani, o cerinţă de asemenea natură va permite actelor să fie transferate în alte sisteme fără a mai fi nevoie să se revizuiască programarea de păstrare şi dispoziţie .*	P
5.1.28.	SMAE trebuie să fie capabil să limiteze administrarea proceselor de dispoziţie doar de către rolul de administrator.	D
5.1.29.	SMAE trebuie sa înregistreze în evidenţa de auditare şi să notifice rolului de administrator toate acţiunile de dispoziţie automate.	D
5.1.30.	SMAE trebuie să notifice rolului de administrator atunci când o acţiune de	D

Ref	Cerinţe	Test
	revizuire trebuie realizată.	
5.1.31.	SMAE trebuie să permită rolului de administrator să delege orice acţiune de revizuire notificată către un rol de revizor pentru acţiune.	D
5.1.32.	SMAE trebuie să permită unui rol de administrator să modifice programarea de păstrare şi dispoziţie (exceptând identificatorul unic, vezi 5.1.6).	D
5.1.33.	Atunci când un rol de administrator mută dosare electronice sau acte între clasele unei scheme de clasificare, SMAE trebuie să ofere opţiunea de a: ▪ permite programării de păstrare şi dispoziţie a clasei de destinaţie să înlocuiască programarea de păstrare şi dispoziţie ; sau ▪ să permită rolului de administrator să selecteze programarea (programărilr) de păstrare şi dispoziţie corespunzătoare. *Aceasta se referă la actele mutate, aşa cum este permis, ca situaţie excepţională, în 8.3.3 şi 8.3.4. În situaţiile rare când această funcţionalitate este folosită, rolurile de administrator vor trebui să fie extrem de atente la atribuirea sau schimbarea programărilor de păstrare şi dispoziţie, în special pentru actele vitale.*	D
5.1.34.	SMAE trebuie să activeze o suspendare a dispoziției, care să fie aplicată unei clase, dosar, sub-dosar sau volum de către rolul de administrator autorizat.	D
5.1.35.	Suspendarea dispoziției nu trebuie să blocheze curgerea sau expirarea unui termen de păstrare. *Cu toate acestea, vezi 5.1.36.*	P
5.1.36.	SMAE trebuie să împiedice ștergerea sau supunerea la oricare altă decizie de dispoziție a oricărei entități și a conținutului său (entități–fiică) supuse unei suspendări de dispoziție. *Ştergerea este descrisă în secţiunea 9.3.*	D
5.1.37.	SMAE trebuie să limiteze în favoarea unui rol de utilizator autorizat dreptul de anulare a unei suspendări de dispoziție.	D
5.1.38.	Atunci când un rol de administrator activează sau anulează o suspendare de dispoziție, SMAE trebuie să captureze şi să stocheze următoarele informaţii despre el, cel puţin în evidenţa de auditare şi de preferat ca metadate: ▪ data la care suspendarea a fost activată sau anulată; ▪ identitatea utilizatorului autorizat; ▪ motivarea pentru suspendare.	D

Ref	Cerinţe	Test
5.1.39.	SMAE ar trebui să permită unui rol autorizat de administrator să aplice mai multe suspendări de dispoziție, fiecare precizând acelaşi motiv, pentru un grup de clase, dosare, sub-dosare sau volume, ca operaţiune în grup. *Această cerinţă permite utilizatorului autorizat să aplice suspendări pentru acelaşi motiv mai multor clase, dosare etc.*	D
5.1.40.	SMAE ar trebui să permită anularea mai multor suspendări de dispoziție (având acelaşi motiv) simultan, ca operaţiune de grup, de către un rol de utilizator autorizat.	D
5.1.41.	SMAE ar trebui să permită unei clase, dosar, sub-dosar sau volum să fie supuse la mai multe suspendări de dispoziție simultane, deoarece ele sunt aplicare entităţii şi/sau pentru că ele sunt aplicatela o entitate de nivel mai înalt. În ambele situaţii, limitările asupra dispoziţiei şi alte funcţionalităţi impuse de suspendarea de dispoziție trebuie să rămână active până când va fi ridicată ultima suspendare de dispoziție care afectează entitatea.	D
5.1.42.	SMAE ar trebui să permită unui utilizator autorizat să caute şi să raporteze toate entităţile supuse unei anumite suspendări de dispoziție.	D
5.1.43.	SMAE poate permite unui utilizator autorizat să seteze, să schimbe şi să şteargă o „notiţă” care înștiințează utilizatorul despre existenţa unei anumite suspendări de dispoziție la o anumită dată.	D

5.2 Revizuirea acţiunilor de dispoziţie

În unele medii, programările de păstrare şi dispoziţie sunt folosite pentru a guverna dispoziţiile fără o revizuire. În altele totuşi, programările de păstrare şi dispoziţie declanşează o revizuire a unor anumite acţiuni de dispoziţie asupra unei clase, dosar etc. atunci când acestea ajung la data sau la evenimentul specificat într-o regulă care i se aplică. Revizuirea poate lua în considerare metadatele, conţinutul sau amândouă în a decide asupra unei acțiuni de dispoziție (un termen de păstrare viitor, transferul în alt sistem, distrugerea sau o combinație a acestora).

Dispoziţia anumitor recorduri este supusă legilor şi reglementărilor. Revizuirea acţiunilor de dispoziţie trebuie să se desfăşoare de o manieră care să fie conformă cu aceste legi şi reglementări, cu orice politică şi proceduri de evaluare stabilite pentru organizaţie şi unde este cazul, în cooperare cu (şi uneori exclusiv de către) autorităţile arhivistice responsabile. Mai multe discuţii despre acest subiect se situează în afara ariei de aplicare a MoReq2.

Ref	Cerinţe	Testabil
5.2.1.	SMAE ar trebui în mod automat să notifice unui rol de administrator toate programările de păstrare şi dispoziţie, care se vor aplica într-o anumită perioadă de timp.	D

Ref	Cerinţe	Testabil
5.2.2.	SMAE trebuie să sprijine procesul de revizuire prin prezentarea claselor, dosarelor, sub-dosarelor şi volumelor ce trebuie revizuite, împreună cu metadatele lor şi informaţiile din programările de păstrare şi dispoziţie. *În practică, acest lucru presupune caracteristici pentru a naviga înainte, înapoi etc. în cadrul şi între dosare şi de la/către metadate pentru dosare şi acte.*	D
5.2.3.	SMAE trebuie să fie capabil să menţină legături între diferite redări ale aceluiaşi act şi să activeze acţiuni de dispoziţie care să fie îndeplinite simultan.	D
5.2.4.	SMAE trebuie să permită revizorului să ia cel puţin una din următoarele acţiuni pentru fiecare clasă, dosar, sub-dosar sau volum în timpul revizuirii: ▪ marcare în vederea distrugerii, imediată sau la o dată viitoare (vezi secțiunea 5.3). ▪ marcare pentru transfer (vezi secțiunea 5.3), imediată sau la o dată viitoare; ▪ marcare pentru o revizuire ulterioare, imediată sau la o dată viitoare; ▪ marcare pentru păstrare nelimitată. *Aceasta poate fi realizată prin aplicarea de diferite programări de păstrare şi dispoziţie sau prin alte mijloace*.	D
5.2.5.	SMAE trebuie să înregistreze automat data revizuirii.	D
5.2.6.	SMAE trebuie să permită revizorului să inserezecomentarii în metadatele clasei, sub-dosarului, volumului sau dosarului pentru a înregistra motivele pentru deciziile de revizuire.	D
5.2.7.	SMAE trebuie să păstreze un istoric nemodificat al tuturor deciziilor luate de către revizor în timpul revizuirii, inclusiv a motivelor. *Deciziile ar trebui să fie stocate ca metadate şi de asemenea să poată fi înregistrate în evidenţa de auditare.*	D
5.2.8.	SMAE ar trebui să alerteze un rol de administrator dacă un conflict apare datorită unui dosar care trebuie distrus şi care este referinţă într-un alt dosar. Trebuie să fie oprit procesul de distrugere pentru a permite luarea următoarelor acţiuni de remediere: ▪ confirmare din partea rolului de administrator de a continua sau de la a anula procesul.	D

Ref	Cerinţe	Testabil
	▪ generarea unui raport care detaliază dosarele sau actul (actele) şi toate referinţele sau legăturile în care este destinaţie.	

5.3 Transfer, export şi distrugere

Organizaţiile pot avea nevoie să mute actele din SMAE spre altă destinaţie sau sistem de arhivare sau alte scopuri. Această acţiune va fi numită în continuare „transfer”.

Motivele pentru transfer pot include:

- păstrare permanentă pentru importanţa de natură juridică, administrativă sau de cercetare a actului;
- folosirea unor servicii separate sau externe pentru managementul documentelor pe termen mediu şi lung.

Această acţiune are adesea ca rezultat transferul actelor către un alt mediu SMAE.

Termenul „transfer” este folosit chiar dacă, iniţial, doar o copie este transmisă la în altă destinaţie sau sistem. Actele rezidente iniţial în SMAE trebuie păstrate şi distruse doar după verificarea măsurii în care dacă transferul a fost de succes.

Termenul „export”, pe de altă parte, se referă la procese de producere a unei copii complete a grupării, dosarelor şi actelor pe un alt sistem, în timp ce actele rămân pe sistemul original – procesul nu le şterge.

În practică, procesul de transfer are loc în două faze — exportul unei copii cu toate metadatele asociate şi evidenţa de auditare cu distrugerea ulterioară a originalului.

La momentul redactării, dezvoltarea unei scheme XML pentru MoReq2 este planificată. Se preconizează ca această schemă să implementeze modelul de metadate MoReq2 şi să furnizeze un protocol ideal pentru transferul actelor electronice între SMAE conforme MoReq2. Deoarece detaliile schemei nu sunt disponibile în momentul redactării, conformitatea cu aceasta nu este cerută.

În orice situaţie, cerinţa este de a executa transferul, exportul sau distrugerea de o manieră controlată. În toate cazurile, în acelaşi timp cu desfăşurarea acţiunilor asupra actelor trebuie luate și decizii despre metadatele şi evidenţa de auditare care se referă la acestea.

În acest context, „distrugere” este diferită de „ştergere”. Ştergerea actelor în alte circumstanţe este acoperită în secţiunea 9.3.

Ref	Cerinţe	Testabil
5.3.1.	Dacă o schemă XML MoReq2 oficială a fost publicată[5], SMAE trebuie să poată exporta acte într-o manieră conformă cu această schemă.	P

[5]La momentul scrierii, dezvoltarea unei scheme XML pentru MoReq2 este pe punctul de a începe. Vezi pentru detalii http://ec.europa.eu/transparency/archival_policy.

Ref	Cerinţe	Testabil
	Vezi de asemenea cerinţa 6.2.1 referitoare la importarea masivă a actelor. Luate împreună, aceste două cerinţe tratează interoperabilitatea SMAE conforme MoReq2.	
5.3.2.	Ori de câte ori un SMAE transferă sau exportă un act, el trebuie să transfere sau să exporte toate componentele şi trebuie să păstreze relaţiile corecte între acestea.	P
5.3.3.	SMAE trebuie să furnizeze un proces bine definit pentru transferul documentelor, împreună cu metadatele asociate şi informaţiile din evidenţa de auditare, către un alt sistem sau către o altă organizaţie.	P
5.3.4.	SMAE ar trebui să poată exporta acte şi metadatele lor sub forma unui pachet de informaţii de transmitere (*SIP, Submission Information Package*), aşa cum este definit de standardul OAIS (vezi anexa 7). *Vezi cerinţa similară pentru pachetul de diseminare a informaţiei (*DIP, Dissemination Information Package*) la 11.7.12.*	D
5.3.5.	Ori de câte ori SMAE transferă vreo clasă, dosar, sub-dosar sau volum, transferul trebuie să includă: ▪ (pentru clase): toate dosarele şi actele din clasă; ▪ (pentru dosare) toate volumele şi sub-dosarele din dosar; ▪ toate actele din toate dosarele, sub-dosarele şi volumele; ▪ toate metadatele sau doar cele selectate asociate cu toate cele de mai sus; ▪ toate evidenţele de auditare sau cele selectate pentru cele de mai sus. *Deşi SMAE trebuie să fie capabil să exporte toate metadatele şi evidenţele de auditare, nu toate acestea sunt întotdeauna cerute de fiecare sistem-ţintă de transfer.*	D
5.3.6.	Ori de câte ori SMAE exportă sau transferă vreun act cu metadatele sale, el trebuie să includă toate metadatele implicite într-o formă explicită. *Altfel spus, toate valorile de metadate care se aplică oricărei clase, dosar, sub-dosar, volum sau act trebuie să fie prezentate explicit, chiar dacă au fost stocate implicit. Vezi anexa 9.3 pentru exemple.*	P
5.3.7.	SMAE trebuie să fie capabil să facă una sau ambele din următoarele acțiuni, atunci când exportă sau transferă vreun set de acte: ▪ exportul sau transferul programărilor de păstrare şi dispoziţie împreună cu actele cărora lise aplică, într-o manieră care să	P

Ref	Cerinţe	Testabil
	permită regulilor să fie re-aplicate actelor în sistemul-destinaţie. ▪ să tipărească unul sau mai multe rapoarte care să arate programările de păstrare şi dispoziţie, care să fie aplicate pentru fiecare set de acte şi caracteristicile acestor programări.	
5.3.8.	SMAE trebuie să fie capabil să facă una sau ambele din următoarele acțiuni la exportarea sau la transferul oricărui set de acte: ▪ exportul sau transferul controalelor de acces împreună cu actele la care se referă, într-o manieră care să permită controalelor să fie reaplicate actelor în sistemul-destinație. ▪ imprimarea unuia sau mai multor rapoarte care să arate controalele de acces aplicabile pentru fiecare set de acte, şi caracteristicile acestor controale.	P
5.3.9.	SMAE trebuie să fie capabil să transfere sau să exporte un dosar sau conţinutul unei clase într-o singură secvenţă de operaţiuni, cum ar fi: ▪ conţinutul şi structura actelor electronice nu sunt schimbate; ▪ toate componentele unui act electronic (atunci când actul constă din mai mult de o componentă) sunt exportate ca o unitate; ▪ toate legăturile dintre act şi metadatele ei şi evidenţă de auditare sunt reţinute. ▪ toate legăturile între clase, dosare, sub-dosare, volume şi acte sunt păstrate astfel încât să fie reconstituite în SMAE care primeşte.	P
5.3.10.	Atunci când SMAE exportă volume şi/sau dosare, dacă oricare volum şi/sau dosar include *pointeri* către acte stocate în alte dosare (vezi 3.4.24), atunci SMAE trebuie să transfere sau să exporte actul complet, nu *pointer*-ul. *Aceasta cerință este impusă astfel încât să existe siguranța că nu există nici o dificultate de redare a pointerului între sistemul de export şi cel de primire.*	D
5.3.11.	SMAE trebuie să fie capabil de a transfera şi exporta acte în formatul în care au fost capturate.	D
5.3.12.	SMAE trebuie să fie capabil de a transfera şi exporta actele în orice format(e) în care actele au fost redate.	D
5.3.13.	SMAE trebuie să furnizeze un utilitar sau un instrument de conversie	P

Ref	Cerinţe	Testabil
	pentru a accepta migrarea actelor marcate pentru transfer sau export într-un format de transfer specificat. *De pildă, un format XML aprobat sau alt format deschis.* *Această cerinţă este destinată sa acopere termene lungi de păstrare, când actele trebuie să fie în mod automat redate într-un format aprobat de prezervare pe termen lung după o perioadă de timp precizată, fără afectarea integrităţii şi autenticităţii actelor.*	
5.3.14.	SMAE trebuie să păstreze toate grupările, actele şi alte informaţii care sunt transferate, cel puţin până când se confirmă succesul procesului de transfer. *Aceasta este o măsură procedurală de siguranță, pentru asigurarea că actele nu sunt distruse înainte ca transferul cu succes să fie raportat de destinatar.*	
5.3.15.	SMAE trebuie să distrugă grupările, actele şi alte informaţii care sunt transferate, atunci când primeşte confirmarea că procesul de transfer este încununat de succes, cu excepția metadateti care este salvată ca urmă. *Vezi 5.3.19*	D
5.3.16.	SMAE ar trebui să exporte întregul conţinut al clasei din schema de clasificare într-o secvenţă de operaţiuni, asigurându-se că: ▪ poziţia relativă a fiecărui dosar în schema de clasificare este menţinută, astfel încât structura de dosare poate fi reconstituită; ▪ sunt păstrate şi mutate odată cu conţinutul clasei metadate suficiente pentru a reconstrui întreaga ramură a clasei mamă.	P
5.3.17.	SMAE ar trebui să furnizeze capacitatea de a adăuga elemente de metadate definite de utilizator cerute pentru scopuri de management arhivistic al dosarelor electronice selectate pentru transfer.	D
5.3.18.	SMAE trebuie să se asigure că toate redările unui act marcat pentru distrugere sunt distruse. *Acolo unde acelaşi act apare în mai mult de un dosar (3.4.24) atunci actul şi redările sale ar trebui să fie scoase din dosar când acesta este distrus, dar nu trebuie să fie şteres definitiv până când toate aparițiile actului nu au fost distruse.*	D
5.3.19.	SMAE trebuie să aibă capacitatea de a păstra urme de metadate (vezi	D

Ref	Cerinţe	Testabil

glosarul) pentru:

- clase
- dosare
- sub-dosare
- volume
- acte stocate direct într-o clasă

care au fost distruse sau transferate.

În anumite medii, este de dorit să se păsteze informaţiile despre acte care au fost distruse. Metadatele în discuţie ar trebui să includă cel puţin data intrării în sistem și toate metadatele relevante care să identifice în mod unic fiecare act și relațiile sale cu schema de clasificare Vezi modelul de metadate MoReq2.

Astfel, organizaţiile pot şti încă ce acte au deţinut şi data la care au fost distruse sau asupra cărora s-a aplicat o acțiune de dispoziție, fără a supraîncărca sistemul prin păstrarea tuturor metadatelor de detaliu pentru dosare şi acte.

5.3.20. Urmele de metadate (vezi 5.3.19) trebuie să includă cel puţin următoarele: D

- data distrugerii sau transferului
- codul complet de clasificare
- titlul
- descrierea
- utilizatorul responsabil pentru distrugere şi transfer
- motivaţia pentru distrugere sau transfer (aceasta poate fi o referinţă la programarea de păstrare şi dispoziţie sau la un motiv introdus manual)

5.3.21. SMAE trebuie să permită unui rol de administrator să specifice un subset de elemente de metadate adiţionale care vor fi reţinute ca urme de metadate. D

5.3.22. SMAE trebuie să poată exporta urmele de metadate atunci când actele sunt exportate. D

Această cerință este impusă pentru a permite migrarea între SMAE.

5.3.23. SMAE trebuie să permită ca informaţiile să fie exportate de mai multe ori. D

Ref	Cerinţe	Testabil
5.3.24.	Ori de câte ori SMAE exportă sau transferă informaţii, ar trebui să fie capabil să producă la cerere un raport, care să cuprindă actele exportate sau transferate în conformitate cu nivelurile lor de securitate.	D

6. Captura şi declararea actelor

Privire generală

Acest capitol prezintă cerinţe referitoare la procesul de captură a actelor într-un SMAE. Prima secţiune (6.1) acoperă procesul obișnuit de captură. Următoarea secţiune (6.2) acoperă importurile masive de acte din alte sisteme, fiind urmată de o secţiune dedicată e-mail-ului, din cauza importanţei sale particulare (6.3). Secţiunea 6.4 tratează genurile de acte şi secţiunea 6.5 acoperă integrarea cu sistemele de scanare şi obţinere de imagini digitale.

Terminologie

Termenul „captură”este folosit şi în alte capitole ale MoReq2. Termenul este folosit în sensul său obișnuit din limba engleză, în contextul tehnologiei informaţiei/managementului informaţiei. În acest context, „captura” informaţiei înseamnă salvarea ei într-un sistem informatic. Aceasta este similară cu sensul arhivistic de „captură”, văzută ca „acţiunea de înregistrare sau salvare a unei anume reprezentări a unui „obiect digital”, aşa cum apare în baza de date terminologică a proiectului InterPares 2 (vezi notă)[6].

Rezultă că SMAE-urile pot captura o varietate de informaţie. Un SMAE poate captura acte, metadate, şi, în unele cazuri documente, printre altele.

Faptul că un SMAE poate (în unele cazuri) captura atât documente, cât şi acte conduce la concluzia inevitabilă că termenul „captură” este imprecis, deoarece captura unui act implică mai multe procese decât captura unui document care nu este un act. De exemplu, captura unui act include procesele de clasificare, înregistrare şi blocare a schimbării, ceea ce nu este în mod necesar cazul pentru documente. Poate din acest motiv, pentru acte termenul „declarare” este uneori folosit ca sinonim cu „captură”; totuşi, termenul „declarare” se poate aplica unui document care începe în afara SMAE, sau unui document care a fost deja capturat ca document de către SMAE.

Această lipsă de precizie ar trebui să aibă vreun impact mic sau deloc asupra clarităţii MoReq2.

Mai multe definiţii oficiale sunt date în glosarele din secţiunea 13.1.

6.1 Captura

Documentele electronice care sunt întocmite sau primite în cursul proceselor de activitate îşi au originea atât în surse interne, cât şi externe. Documentele electronice vor fi în formate variate, vor fi produse de diferiţi autori şi pot vor fi primite atât ca documente singulare, cât şi ca documente

[6]vezi http://www.interpares.org/ip2/ip2_terminology_db.cfm

formate din mai mult componente (vezi glosarul pentru definiţia „componentei” în contextul MoReq2).

Unele acte sunt create în cadrul organizaţiei, în cursul proceselor de activitate. Alte sunt primite prin canale de comunicaţie variate, de pildă poştă electronică, fax, corespondența poştală (ce poate fi opţional scanată), prin înmânareşi la volume și rate de sosire variabile. Pentru a captura documente este nevoie de un sistem flexibil de captură cu bune comenzi de management și ca urmare diverse cerinţe sunt tratate.

Re	Cerinţe	Testabil
6.3.1	Procesul de captură al unui SMAE trebuie să furnizeze comenzile şi funcţionalităţile care să permită utilizatorilor să: ▪ captureze actele electronice indiferent de formatul fişierului, metodă de codificare sau alte caracteristici tehnologice, fără alterarea conţinutului; ▪ să se asigure că actele sunt asociate unei scheme de clasificare; ▪ să se asigure că actele sunt asociate cu unul sau mai multe dosare. *„Formatul de fişier” este definit în glosar. Cerinţa este de a fi capabil să captureze orice format de fişier.* *Nu se urmărește ca cerinţa de a captura acte în orice format să fie testabilă şi nu implică necesitatea ca SMAE să poată prezenta (vezi glosarul) toate formatele posibile. MoReq2 prin urmare nu listează tipurile de formate care ar putea fi capturate, deoarece formatele pot varia în timp odată cu evoluţia software-ului. Totuşi, pentru a evita dubiul, felurile de acte care trebuie incluse pot fi diverse; ele ar putea include, de pildă, următoarele feluri de acte, frecvent utilizate în setările tip office:* ▪ *rezultate de la aplicaţii desktop de tipul pachetelor office;* ▪ *e-mailuri (vezi secţiunea 6.3)* ▪ *audio* ▪ *baze de date* ▪ *pdf* ▪ *imagini scanate* ▪ *video* ▪ *pagini web* *În anumite situaţii, SMAE poate de asemenea să captureze alte feluri de*	P

Re	Cerinţe	Testabil

acte, cum ar fi:

- *bloguri;*
- *fişiere compresate (uneori menționate sub denumirea de „arhive", în sensul IT al termenului);*
- *calendare electronice;*
- *formulare electronice;*
- *date GIS;*
- *informaţii din alte aplicaţii computerizate, de pildă contabilitate, state de plată, proiectare asistată de calculator;*
- *sisteme de mesagerie instantanee;*
- *înregistrări ale tranzacţiilor web;*
- *acte care includ legături către alte acte;*
- *codul sursă al unor softuri şi documentaţia de proiect;*
- *date structurate (de pildă tranzacţii EDI);*
- *transmisii web*
- *wiki*

Aceste liste nu sunt complete.

6.3.2 SMAE nu trebuie să impună nici o limită practică a numărului de acte care pot fi capturate în orice clasă, dosar, sub-dosar sau volum, nici asupra numărului de acte care pot fi stocate în SMAE. P

Numărul mare de acte în volume etc. va avea tendinţa de a face sistemul dificil de utilizat în anumite setări şi prin urmare acest lucru nu este în general recomandat. Această cerinţă urmărește să permită situaţiile în care un numărul mare este de neevitat, cum ar fi anumite medii tranzacţionale.

6.3.3 La captura unui act alcătuit din mai multe componente (vezi glosarul), SMAE trebuie sa captureze toate componentele sale. P

6.3.4 La captura actelor electronice care au mai mult de o componentă, SMAE trebuie să permită ca actul să fie administrat ca o singură unitate, reţinând relaţia între componente şi păstrând integritatea structurală a actului. P

Exemple de asemenea acte sunt:

- *pagini web cu elemente grafice încorporate*
- *un document realizat cu un procesor de texte legat de o foaie*

Re	Cerinţe	Testabil

de calcul.

În unele cazuri, componentele vor fi conectate prin legături care nu vor funcţiona dacă vor fi pur şi simplu copiate într-un depozit SMAE. De pildă, multe pagini web conţin legături către grafice şi alte obiecte cu adrese (URL-uri) exterioare depozitului; şi foile de calcul legate conţin, în mod obişnuit, legături către adrese (nume de fişiere ale sistemului de operare) externe depozitului. Vezi cerinţa următoare.

6.3.5 La capturarea unui act electronic ce are mai mult de o componentă, SMAE ar trebui să modifice actul, dacă este necesar, pentru a păstra posibilitatea de a-l prezenta. Aceasta va însemna probabil ca SMAE să modifice referinţele (legăturile) interne între unele componente. P

Această cerinţă se aplică doar formatelor de fişiere specificate pentru SMAE — nu se urmărește să se aplice pentru formatele nespecificate. Exemple ar putea include:

- *pagini HTML care includ legături către grafice sau alte obiecte;*
- *foi de calcul tabelar care includ legături către alte foi de calcul.*

Realizarea acestor schimbări este contrară principiului general de a nu schimbă conţinutul actului, dar este inevitabilă dacă actul care include componente etc. trebuie să fie stocat în formatul său original, fără pierderea tuturor funcţionalităţilor şi acurateţei. Schimbările vor fi în general acceptate atât timp cât toate schimbările sunt înregistrate în evidenţa de auditare a SMAE (vezi cerinţa următoare). O abordare alternativă implică redarea actului în alte formate de fişiere (cum ar fi PDF/A) care păstrează imaginea statică; vezi cerința 11.7.8; totuşi, chiar dacă aceasta evită schimbarea legăturilor, este probabil că efectul va fi pierderea lor.

6.3.6 Atunci când SMAE schimbă referinţele în cadrul actelor în timpul capturii, el trebuie să înregistreze automat toate detaliile schimbărilor făcute în evidenţa sa de auditare. D

6.3.7 SMAE trebuie să captureze automat formatul de fişier (vezi glosarul), incluzând versiunea fiecărei componente, atunci când e capturată şi trebuie o stocheze în metadatele componentelor actului. P

Aceasta este cerută pentru a accepta păstrarea digitală a actelor — accesibilitatea lor în timp. Vezi secţiunea 11.7.

Unele informaţii despre formatul de fişier sunt în mod obişnuit implicite în extensia numelui de fişier al componentei, de pildă „.htm”, sau „.pdf”. Totuşi, doar extensia nu indică versiunea formatului de fişier. Aceasta va

Re	Cerinţe	Testabil
	fi acceptabilă în multe cazuri, deşi ar putea să nu fie suficientă în situaţiile în care există necesitatea unei păstrări pe termen lung sau unde este nevoie de precizie (de pildă, precizia spaţiului de culoare). *Formatele de fişiere sunt numeroase şi supuse unei frecvente schimbări. Prin urmare, nu este realistă aşteptarea ca un SMAE să captureze informaţiile pentru toate formatele de fişiere. Este prin urmare acceptabil pentru un SMAE să:* ▪ *specifice o listă a formatelor care pot fi recunoscute;* ▪ *să se bazeze pe o referire la un registru prestabilit de formate de fişiere — de preferat unul proiectat special pentru a sprijini păstrarea digitală.* *În ambele cazuri, organizaţia utilizatoare trebuie să se asigure că seria de formate de fişiere inclusă este suficientă pentru cerinţele ei de păstrare.*	
6.3.8	Atunci când actele sunt capturate, procesul SMAE de captură al actelor trebuie să valideze valorile metadatelor intrate în SMAE, la un minim conform cu regulile din modelul de metadate MoReq2. *Vezi de asemenea 6.3.34 în această secţiune.*	D
6.3.9	SMAE ar trebui să accepte validarea elementelor de metadate folosind algoritmi de sumă de control. *De exemplu, fişierele pot fi identificate printr-un număr de tip card de credit de 16 digiţi, dintre care ultimul digit este un digit de control calculat din ceilalţi 15 digiţi, folosind algoritm decimal.* *În mod normal, ar trebui să se accepte existența prevederilor pentru o interfaţă a unei aplicaţii pentru această caracteristică, care să permită organizaţiilor să îşi introducă propriul algoritm ales.*	D
6.3.10	SMAE trebuie să permită utilizatorilor să captureze un act electronic chiar dacă aplicaţia folosită pentru a produce actul nu este prezentă. *De pildă, un utilizator poate primi un plan de proiect şi desene CAD/CAM ca anexe ale unui e-mail. Dacă utilizatorul nu are acces la aplicaţiile pentru planul de proiect sau CAD/CAM, atunci utilizatorul nu ar putea să vizualizeze anexele. În ciuda acestui fapt, utilizatorul ar trebui să fie capabil să captureze anexele ca acte în SMAE. SMAE poate furniza softuri de vizualizare care să permită utilizatorului să vizualizeze aceste acte; aceasta nu este cerută de MoReq2.*	D
6.3.11	SMAE trebuie să fie capabil să captureze metadate despre acte conform cu modelul de metadate MoReq2.	D

Re	Cerinţe	Testabil
6.3.12	SMAE ar trebui să fie capabil să captureze automat valori din câmpurile definite de un rol de administrator în cadrul genurilor de documente precizate, folosind aceste valori automat pentru a popula elementele de metadate, aşa cum sunt specificate în modelul metadate MoReq2. *Funcţionalitatea necesară pentru această cerinţă se aplică doar pentru obiectele electronice care au o structură internă predictibilă, de exemplu scrisori produse folosind anumite şabloane şi un anume procesor de text.* *Multe documente, incluzând unele documente tip office sau şi fişiere .PDF, includ elemente de metadate configurabile de către utilizator. Ar trebui ca SMAE să poată fi configurat să captureze automat valorile acestor elemente ş să le păsteze împreună cu actul.*	D
6.3.13	SMAE trebuie în orice moment să permită captura elementelor de metadate specificate la configurarea sistemului şi trebuie să le păstreze într-o relaţie de legătură permanentă cu actul electronic.	D
6.3.14	SMAE ar trebui să permită utilizatorilor care doresc să captureze un act, dar care nu au capacitatea de a furniza toate metadatele obligatorii pentru el, să îl stocheze temporar în SMAE. *Altfel spus, SMAE ar trebui să furnizeze mijloace pentru stocarea actelor fără toate metadatele lor, adică fără a încheia procesul normal de captură. Aceasta implică raportarea excepţiilor şi monitorizarea progresului; nu implică nici o cerinţă de a trata aceste acte ca acte normale pentru scopuri de export, transfer, redare etc. MoReq2 nu specifică cum se poate realiza acest lucru.* *Doar valorile de metadate editabile pot fi schimbate la un moment viitor, iar metadatele fixe (de ex., datele de transmitere a e-mail-ului) trebuie să rămână neschimbate.*	D
6.3.15	SMAE trebuie să se asigure că valorile unor elemente de metadate ale actelor electronice pot să fie actualizate doar de către utilizatorii autorizaţi sau de către rolurile de administrator, conforme cu regulile din capitolul 12.	D
6.3.16	SMAE trebuie să se asigure că tuturor actelor le este atribuită în momentul capturii cel puţin o clasă, un dosar (sau sub-dosarul său, dacă e cazul), după cum este cazul.	D
6.3.17	SMAE ar trebui să accepte asistenţă automată în captura documentelor electronice, prin extragerea automată a câtor mai multe metadate posibile, pentru cât mai multe formate de fișiere posibile.	N

Re	Cerinţe	Testabil

Motivarea pentru această cerinţă este acea de a:

- *minimiza cantitatea de intrări de date realizată de către utilizatori (experienţa arată că în multe medii, o cerinţă de a introduce metadatele poate determina utilizatorii să respingă sistemul);*
- *spori acurateţea metadatelor.*

Elementele de metadate implicate, şi felurile de documente pentru care este posibil, vor depinde de mediu. Unele indicații sunt date în modelul de metadate.

6.3.18 SMAE trebuie să accepte asistenţă automată în captura documentelor care ies şi a celor interne (note, scrisori din procesoarele de texte într-un layout şi un format de fişier precizat) ca acte, prin extragerea automată a următoarelor metadate din ele: D

- data documentului (cum apare în corpul documentului);
- destinatar(i);
- destinatar(i) secundar(i);
- linia de subiect (titlul);
- autor(i);
- referinţa internă (de obicei prezentată ca „referinţa noastră”),

în măsură în care acestea sunt prezente.

MoReq2 nu specifică software-ul sau formatul pentru documente sau e-mail-uri tip office. Extragerea de metadate poate fi realizată prin localizarea metadatelor în cadrul actului, prin folosirea unui şablon pentru a identifica metadatele şi pentru a scrie un document necompletat, sau prin orice alte mijloace.

6.3.19 SMAE trebuie să captureze data şi ora unui act, atât ca metadate, cât şi în evidenţa de auditare. D

Dacă data şi ora sunt parte a identificatorului unic al actului, şi atât timp cât acestea pot fi extrase în mod explicit din acest număr, ar putea să nu fie necesar să se stocheze data şi ora separat.

MoReq2 nu specifică acurateţea necesară pentru oră. Cele mai multe SMAE înregistrează ora cu o acurateţe de o secundă sau mai mult.

Unele cadre legislative solicită ca marcarea orei să fie realizată în conformitate cu un anumit dispozitiv sau referință certificată. Acolo unde este cazul, acest lucru trebuie precizat în Capitolul Zero.

Re	Cerinţe	Testabil
6.3.20	Pentru orice act capturat, SMAE trebuie să fie capabil de a prezenta pe ecran metadatele, incluzându-le pe cele de precizate în momentul configurării sistemului. *Metadatele specificate în momentul configurării sistemului pot consta din câteva sau din toate elementele din secţiunea relevantă a capitolului 12.*	D
6.3.21	SMAE trebuie să se asigure că toate metadatele obligatorii sunt prezente pentru fiecare act capturat.	D
6.3.22	În timpul capturii unui act, SMAE trebuie să ceară utilizatorului să introducă orice metadate cerute care nu au fost capturate automat.	D
6.3.23	SMAE trebuie să accepte atribuirea de cuvinte-cheie multiple (sau termeni cheie) pentru fiecare clasă, dosar, sub-dosar şi act. *MoReq2 nu solicită posibilitatea de atribuire a cuvintelor cheie pentru volume.*	D
6.3.24	SMAE ar trebui să permită unui rol de administrator să configureze în ce măsură cuvintele cheie sunt obligatorii sau opţionale, în momentul configurării sistemului, pentru fiecare clasă, dosar sau sub-dosar.	D
6.3.25	SMAE trebuie să permită să fie creată mai mult de o entitate (clasă, dosar etc., folosind aceeaşi combinaţie de cuvinte cheie.	D
6.3.26	SMAE ar trebui să permită unui utilizator să creeze, printr-o singură acţiune, o entitate, pentru a o popula cu valorile sale de cuvinte cheie, prin copierea lor integrală din altă entitate.	D
6.3.27	SMAE ar trebui să permită utilizatorului să introducă un identificator pentru una sau mai multe limbi, pentru orice act.	D
6.3.28	SMAE trebuie să furnizeze posibilitatea ca valorile cuvintelor-cheie sau alte valori ale elementelor de metadate să fie preluate din sau verificate cu un vocabular controlat (sau listă de termeni permişi). *De pildă, prin intermediul unei liste de opțiuni sau tezaur. Vezi de asemenea cerința 11.8.11.*	D
6.3.29	SMAE trebuie să permită introducerea unor alte metadate descriptive sau de alt tip, la momentul capturii şi/sau la un stadiu ulterior al prelucrării.	D
6.3.30	SMAE trebuie să avertizeze utilizatorul daca s-a produs vreo încercare de a captura un obiect cu un titlu care există deja în aceeaşi entitate sau să	D

Re	Cerinţe	Testabil
	redenumească un obiect cu un titlu care deja există în aceeaşi entitate. *Vezi de asemenea 11.8.6.*	
6.3.31	SMAE trebuie să fie capabil să rezerve posibilitatea de a modifica titlul unui act electronic pentru rolul de administrator sau pentru alt utilizator autorizat. *Această facilitate poate sau nu să fie folosită, la opţiunea organizaţiei.*	D
6.3.32	Atunci când un utilizator capturează un document care are mai mult de o versiune, SMAE trebuie să permită utilizatorului să aleagă cel puţin una din următoarele: ▪ să declare toate versiunile ca un singur act; ▪ să declare o versiune specificată ca act; ▪ să declare fiecare versiune ca un act individual.	D
6.3.33	SMAE ar trebui să fie capabil să furnizeze un sprijin automat pentru deciziile de clasificare a actelor electronice, prin mijlocirea cel puţin uneia din următoarele: ▪ realizarea doar a unui subset al schemei de clasificare accesibil unui utilizator sau rol; ▪ sugerarea claselor sau dosarelor folosite cel mai recent de acel utilizator; ▪ sugerarea claselor sau dosarelor folosite cel mai frecvent de acel utilizator; ▪ sugerarea claselor sau dosarelor prin deducere din elementele de metadate ale actului. (de pildă, cuvinte semnificative folosite în titlu sau în rândul de subiect a e-mailului); ▪ sugerarea claselor sau dosarelor prin deducere din conţinutul actului.	P
6.3.34	SMAE ar trebui să permită ca procesul de captură să fie încheiat de mai mult decât un utilizator. *SMAE ar trebui să permită ca procesul de captură să fie împărţit între utilizatori; în mod obişnuit, aceasta va semnifica faptul că un utilizator va introduce unele metadate şi apoi transferă actul electronic către alt utilizator, care introduce metadatele rămase şi clasează actul.*	D
6.3.35	SMAE ar trebui să furnizeze facilităţi elementare de flux de lucru, pentru a activa dirijarea simplă de verificare şi aprobare a unui document anterior capturii, înregistrarea deciziilor luate, cine le-a luat şi să permită	D

Re	Cerinţe	Testabil
	introducerea de către fiecare a motivaţiei. *De remarcat faptul că se cer doar caracteristici elementare de flux de lucru. În mod intenţionat s-a restrâns faţă de caracteristicile totale de flux de lucru descrise în capitolul 10.*	
6.3.36	SMAE ar trebui să furnizeze o interfaţă de programare a aplicaţiei pentru a primi şi captura în timp real acte individuale şi tranzacţii furnizate de o altă aplicaţie sau de un alt sistem. *Aşa cum este menţionat în secţiunea 1.4, funcţionalitatea de management al actelor electronice poate fi cerută ca parte a unui sistem mai larg. Acest lucru ar putea solicita ca SMAE să primească acte din alt sistem, de pildă, o aplicaţie pentru activitatea organizațiilor (corporate business application), cum ar fi managementul relaţiilor cu clienţii (Customer Relationship Management, CRM) sau o linie de aplicaţii de afaceri prin intermediul unei Interfeţe de programare a aplicaţiei (Application Programming Interface, API) pentru a seta SMAE să captureze actele individuale.*	N
6.3.37	Acolo unde este posibil, SMAE ar trebui să emită un avertisment dacă un utilizator încearcă să captureze un act e-mail care a fost deja capturat în acelaşi dosar sau (dacă este clasat direct într-o clasă) în aceeaşi clasă. *MoReq2 nu defineşte cum e-mail-ul este identificat; cu toate acestea, ID de internet al mesajului poate fi potrivit.* *Există câteva cazuri în care nu este logic posibil, de pildă, atunci când actul e-mail a fost capturat într-un fișier la care utilizatorul nu are acces.*	D
6.3.38	Acolo unde este posibil, SMAE ar trebui să emită un avertisment dacă un utilizator încearcă să captureze un act (altul decât un e-mail, aşa cum este tratat de 6.3.37) care are acelaşi conţinut cu un alt act care a fost deja înregistrat în acelaşi dosar sau (dacă este clasat direct într-o clasă) în aceeaşi clasă.	D
6.3.39	Acolo unde este posibil, SMAE ar trebui să emită un avertisment dacă un utilizator încearcă să captureze un act (altul decât un e-mail, aşa cum este tratat de 6.3.37) care are aceleaşi valori ale metadatelor de identificar ca un alt act care a fost deja înregistrat în acelaşi dosar sau (dacă este clasat direct într-o clasă) în aceeaşi clasă. *Metadatele de identificare pentru această cerinţă sunt:* ▪ *titlul* ▪ *data*	D

Re	Cerinţe	Testabil
	▪ *autor* ▪ *destinatar*	
6.3.40	Acolo unde este posibil şi corespunzător, SMAE ar trebui să furnizeze o atenţionare, dacă o încercare este făcută de a captura un act care este incomplet sau inconsecvent de o manieră care va compromite viitoare sa credibilitate aparentă. *De pildă, un ordin de cumpărare fără o semnătura electronică valabilă sau o factură de la un furnizor necunoscut.*	N
6.3.41	SMAE trebuie să permită unui rol de administrator (şi nu unui rol de utilizator) să adauge acte unui volum închis anterior, dacă actului nu este ulterioară datei închiderii. Atunci când acest lucru se întâmpla: ▪ SMAE trebuie să solicite ca un rol de administrator să adauge un motiv, atât în metadatele volumului, cât şi în cele ale actului, pentru a explica de ce această excepţie s-a produs; ▪ SMAE trebuie să înregistreze automat această situaţie în evidenţa de auditare. ▪ acţiunea nu trebuie să actualizeze data închiderii stocată în metadate. *Aceasta posibilitate este destinată folosirii pentru a corecta erori de utilizator, de ex. dacă un volum a fost închis neintenţionat. Din acest motiv, este important ca excepţia care a declanşat această acţiune să fie documentată corespunzător.* *MoReq2 nu impune cum să fie realizată acestă cerinţă. Ea poate fi realizată prin re-deschiderea temporară a unui volum închis sau prin alte mijloace.*	D

6.2. Importarea masivă

Actele pot ajunge masiv într-un SMAE prin mai multe modalităţi. De pildă:

- transfer masiv dintr-un SMDE compatibil
- transfer masiv dintr-un SMAE compatibil
- ca un singur fişier de date compatibil conţinând o serie de acte de acelaşi gen (de ex., facturi zilnice)
- dintr-un sistem compatibil de scanare sau generare de imagini digitale.
- acte dintr-o ierarhie de directoare ale sistemului de operare.

SMAE trebuie să le poată accepta şi trebuie să includă caracteristici pentru a administra procesul de captură şi pentru a păstra conţinutul şi structura actelor importate.

În timpul importului masiv, SMAE trebuie să captureze aceeaşi informaţie ca şi procesul normal de captură — respectiv actele înseşi şi metadatele lor. Trebuie de asemenea să clasifice actele — extinzând schema de clasificare, dacă este necesar (vezi 3.1.12) — şi, posibil, să captureze informaţii în evidenţa de auditare. În fine, importul masiv trebuie să permită procesarea excepţiilor şi erorilor.

În momentul redactării, este planificată dezvoltarea unei scheme XML pentru MoReq2. De la această schemă se aşteaptă să implementeze modelul de metadate MoReq2 şi să furnizeze un protocol ideal pentru importul masiv a actelor electronice dintr-un SAME, conform MoReq2. Deoarece detaliile schemei nu sunt disponibile în momentul redactării, conformitatea cu ea nu este cerută.

Ref	Cerinţe	Testabil
6.2.1.	Dacă o schemă XML MoReq2 oficială a fost publicată, SMAE trebuie să poată desfăşura o importare masivă de acte de o manieră conformă cu această schemă. *Vezi de asemenea cerinţa 5.3.1 referitoare la exportarea actelor. Luate împreună, aceste două cerinţe tratează interoperabilitatea sistemelor conforme MoReq2.*	P
6.2.2.	SMAE trebuie să furnizeze capacitatea de a captura înregistrările de tranzacţie generate de alte sisteme. Aceasta poate include: ▪ să accepte importări în loturi ale fişierelor de tranzacţie ▪ să furnizeze reguli editabile pentru a personaliza captura automată a actelor; ▪ validarea pentru a menţine integritatea datelor. *MoReq2 nu specifică modul în care este furnizată această posibilitate.*	P
6.2.3.	SAE trebuie să fie capabil să captureze automat în timpul importului masiv metadatele asociate cu actele (permiţând introducerea manuală a metadatelor care lipsesc sau sunt incorecte).	P
6.2.4.	Acolo unde SMAE capturează metadatele unor acte în timpul importului, trebuie să le valideze folosind aceleaşi reguli care ar fi folosite pentru captura manuală a actelor. Acolo unde un proces de validare găseşte erori (cum ar fi absenţa metadatelor obligatorii sau erori de format) el trebuie să le aducă în atenţia utilizatorului care desfăşoară importarea, în toate cazurile identificând metadatele implicate şi înregistrând erorile şi acţiunile în evidenţa de auditare.	D

Ref	Cerinţe	Testabil

În cazurile ideale, actele care sunt importate vor avea metadate care sunt în totalitate conforme cu modelul de metadate. În alte cazuri, metadatele pot să fie neconforme. În aceste cazuri, câteva soluţii sunt posibile; MoReq2nu obligă la nici una dintre ele. Posibilele soluţii sunt:

- *întreaga importare este anulată;*
- *importarea actului care are metadate neconforme este anulată*
- *utilizatorul este solicitat să aleagă între corectarea erorii şi anularea importării clasei afectate*.

Datele sunt importate ca acte incomplete temporar (aceasta se referă la cerinţa după care captura poate fi împărţită între utilizatori, vezi 6.3.34).

6.2.5. SMAE trebuie să fie capabil să importe evidența de auditare care prezintă istoricul actelor importate. D

6.2.6. SMAE trebuie să nu importe înregistrările evidenţei de auditare în noua evidenţă de auditare; trebuie să importe înregistrările evidenţei de auditare ca un act separat. D

Evidenţa de auditare ca act trebuie să fie păstrată separat, astfel încât să evite producerea de mecanisme care să permită rolurilor administrative să schimbe sau să compromită integritatea evidenţei de auditare. MoReq2 nu specifică cum se poate realiza acest lucru; poate implica stocarea evidenţei de auditare importate ca act alături de actele importate sau ca entitate separată, recunoscută ca o evidenţă de audit importată din alt sistem.

SMAE trebuie să furnizeze posibilităţi de a administra cozile de intrare. D

Se au în vedere următoarele facilităţi:

- *vizualizarea cozii*
- *oprirea temporară a oricăreia sau a tuturor cozilor*
- *re-pornirea uneia sau a tuturor cozilor*
- *ştergerea unei cozi.*

6.2.7. SMAE trebuie să abiliteze un rol de administrator să seteze (opţional) SMAE să închidă clasele, dosarele şi volumele în mod automat după ce au fost importate. D

De pildă, la fuziunea a două organizaţii poate fi necesar să se închidă ramuri ale unei structuri astfel încât să nu mai poată fi adăugate acte la ele.

6.3 Managementul mesageriei electronice (e-mail-urilor)

Definiţii

Ca verb, „[a transmite un] e-mail”[7] se referă la un mecanism de transmitere a mesajelor între „agenţi” (în acest context, termenul „agent” are un sens tehnic specific; mai multe detalii nu sunt cerute pentru înţelegerea MoReq2).

Protocolul standard folosit pentru transmiterea de e-mail-uri este definit de documentele RFC 2821 şi RFC 2822 ale Network Working Group. MoReq2 foloseşte RFC 2821/RFC 2822 ca fundament al definiţiei de lucru pentru „transmiterea de e-mail-uri”.

Ca substantiv, „e-mail" este de obicei folosit pentru a face referire la un document capturat de un agent care conţine datele complete ale unei singure transmisii. Cu toate acestea, deşi RFC 2822 defineşte sintaxa pentru transmisiunile e-mail, nu există standarde care să definească formatul de date şi care ar trebui folosit atunci când transmisia e-mail sunt capturate la documente.

Altfel spus, chiar dacă aplicaţiile de e-mail de la diferiţi furnizori pot transmite liber mesaje între ele (deoarece pot respecta protocoalele de e-mail definite în RFC 2821/RFC 2822) nu este posibil să capturezi o transmisie e-mail de la o aplicaţie e-mail ca un document şi să garantezi că altă aplicaţie e-mail va fi capabilă să îl citească, atât timp cât fiecare furnizor de email respectă propriul format brevetat pentru captura e-mail-ului. În mod similar, extragerea automată de metadate din mesaje nu poate fi garantată.

Folosire și aspecte

E-mail-ul este folosit pentru a trimite documente (sub formă de mesaje şi de anexe) în cadrul şi între organizaţii. Caracteristica softurilor de administrare a e-mail-urilor (în special lipsa standardizării formatelor explicată mai sus), combinată cu atitudinea utilizatorilor faţă de e-mail-uri, poate face dificilă aplicarea de funcţionalităţi pentru acestea. Organizaţiile trebuie fie capabile să implementeze controale de procedură şi de administrare pentru:

- captura tuturor mesajelor şi anexelor lor, intrate şi ieşite

şi/sau să:

- captureze e-mailuri şi anexe în conformitate cu reguli predefinite

şi/sau să:

- furnizeze utilizatorilor capacitatea de a captura mesajele şi anexele selectate.

În unele State Membre europene, proprietatea juridică a e-mail-urilor este neclară şi în unele cazuri, captura automată a e-mail-urilor într-un SMAE poate să nu corespundă cadrului legal. Acolo unde se consideră că este cazul, ultimele două opţiuni ar trebui luate în considerare pentru configurare.

Mai mult, e-mail-urile au devenit principal standard de comunicaţie pentru multe organizaţii şi unul important pentru altele. În unele organizaţii, mult din traficul de e--mail este efemer. Fiecare

[7] În limba engleză, e-mail poate fi atât substantive, cât și verb (n.tr.)

organizaţie are nevoie să decidă care din abordările de mai sus reprezintă cel mai cuvenit compromis pentru situaţia sa:

- prima opţiune presupune captura oricărui e-mail efemer, cât şi cele care sunt acte semnificative.
- a doua opţiune presupune configurarea cu succes a regulilor şi filtrelor potrivite;
- a treia opţiune cere ca utilizatorii să stabilească relevanţa şi importanţa pieselor şi există riscul ca el sa nu poată face acest lucru credibil.

MoReq2 permite ca SMAE să accepte toate cele 3 abordări. Controlul procedurilor şi administrării nu formează obiectul MoReq2.

Ref	Cerinţe	Testabil
6.3.1.	Ori de câte ori un e-mail este capturat, SMAE trebuie implicit să îl captureze într-un format care îi reţine şi informaţiile din antet (*header*).	D
6.3.2.	SMAE trebuie să captureze e-mail-urile într-o manieră integrată, respectiv astfel încât captura să fie realizată de utilizator din aplicaţia de e-mail, fără a fi nevoie ca utilizatorul să comute pe SMAE. *MoReq2 permite de asemenea, dar nu cere, captura e-mail-urilor în alte modalităţi, mai puţin strâns integrate.*	D
6.3.3	Trebuie să fie posibil să se configureze un SMAE în momentul configurării sistemului, astfel încât să opereze în una din următoarele modalităţi, atunci când un utilizator trimite un e-mail: ▪ capturează automat e-mail-ul; ▪ stabileşte dacă să captureze e-mail-ul conform unor reguli predefinite; ▪ avertizează utilizatorul în mod automat, dându-i acestuia opţiunea de a captura e-mail-ul. ▪ nu ia nici o acţiune (şi se bazează pe utilizator că va iniţia captura dacă se cuvine). *Indiferent de ce modalitate este aleasă, este acceptabil pentru un SMAE să ceară utilizatorului să clasifice manual actele şi să introducă manual anumite metadate.*	D
6.3.4.	Trebuie să fie posibil să fie configurat un SMAE în momentul configurării sistemului, astfel încât să opereze în una din următoarele modalităţi, atunci când un utilizator de SMAE primeşte un e-mail: ▪ capturează automat mesajul, dacă acesta nu a fost deja capturat; ▪ hotărăşte dacă să captureze e-mail-ul în conformitate cu reguli	D

Ref	Cerinţe	Testabil

predefinite;

- dacă e-mail-ul nu a fost deja capturat, îl avertizează automat pe utilizator, dându-i acestuia opţiunea de a-l captura;
- nu iniţiază nici o acţiune (şi astfel se bazează pe utilizator să iniţieze captura dacă se cuvine).

Indiferent de care cale este aleasă, se acceptă ca SMAE sa ceară utilizatorului să clasifice actele manual şi să adauge metadatele manual.

6.3.5. SMAE trebuie să accepte asistenţa automată în captura e-mail-urile intrate şi ieşite, cu sau fără anexe, ca acte, prin extragerea automată a următoarelor metadate din acestea: P

- data (şi în unele setări ora) trimiterii mesajului;
- destinatar(i);
- destinatari secundari;
- rândul de subiect (titlul);
- destinatar;
- semnătura electronică încorporată;
- furnizorul de serviciu de certificare

în măsura în care acestea sunt prezente.

Această cerinţă specifică captura „emitenţilor" pentru mesaje e-mail-uri. Acesta nu este întotdeauna identic cu autorul, de pildă, atunci când o secretară trimite un mesaj în numele unui director. Captura „emitentului" este specificată aici ca un compromis conştient, fiind imposibil de a captura autorul, de o manieră credibilă, în mod automat. Organizaţiile ar trebui să ia în considerare nevoia de proceduri manuale pentru a asigura corectitudinea metadatei de identificare a autorului.

6.3.6. Utilizatorii ar trebui să fie capabili să tranfere un act e-mail către un sub-dosar, dosar sau clasă prin tragerea lui din clientul de e-mail (tehnic, un Agent al Utilizatorului de Mail) către un anume sub-dosar, dosar sau clasă în SMAE. D

Sub-dosarul, dosarul sau clasa pot fi reprezentate în fereastra clientului de e-mail sau într-o fereastră separată.

6.3.7. SMAE trebuie să permită unui utilizator să aleagă cum să captureze un mesaj e-mail cu anexe: D

- doar mesajul e-mail, fără anexe;
- e-mail-ul, cu anexele sale, ca un act format din componente

Ref	Cerinţe	Testabil
	legate; ▪ doar anexa(ele), fiecare sau oricare ca acte individuale. *Aceasta se aplică la transmiterea şi primirea mesajelor.* *Ultima din aceste trei opţiuni presupune ca anexa(ele) să fie capturate fără contextul e-mail-urilor cu care au fost transmise.*	
6.3.8.	Acolo unde e-mail-ul şi anexele sunt capturate în acelaşi timp, dar ca acte separate, actele rezultante ar trebui să fie legate automat prin SMAE. *SMAE trebuie să permită utilizatorului să navigheze prin intermediul referinţei încrucişate între acte, astfel încât să descopere fiecare anexa act din actul e-mail şi e-mailul act din actul anexă.*	D
6.3.9.	Ori de câte ori o anexă este capturată ca act separat, SMAE trebuie să solicite ca valorile corespunzătoare metadatelor actului să fie capturate şi/sau introduse pentru el.	D
6.3.10.	La captura unui mesaj e-mail, SMAE trebuie să populeze implicit metadata Titlu cu câmpul „subiect” al mesajului. *Anexa 9 oferă indicații despre interpretarea metadatelor e-mail-urilor.*	D
6.3.11.	SMAE trebuie să permită utilizatorului care capturează un mesaj e-mail să completeze titlul actului. *Aceasta are ca scop să permită utilizatorilor să corecteze titlurile necorespunzătoare sau să clarifice titlurile e-mail-urilor sau să facă titlurile mai semnificative.* *Titlul e-mail-ului este separat de rândul de subiect (titlul) al e-mail-ului; ultimul va rămâne ca parte a mesajului indiferent de conţinutul titlului e-mail-ului.*	D
6.3.12.	Dacă un utilizator capturează un raport de notificare a situaţiei de transmitere a e-mail-ului (acolo unde acestea sunt acceptate) pentru un e-mail care a fost capturat ca act, SMAE ar trebui să fie capabil să le lege automat pe cele două. *Exemple de notificări a situației de transmitere sunt rapoartele de ne-transmitere şi confirmările de transmitere. Aceste legături (*link*) ar trebui să permită utilizatorului să navigheze între acte astfel încât să descopere fiecare notificare de la e-mail-ul act, şi e-mail-ul act de la orice notificare.*	D
6.3.13.	SMAE trebuie să activeze captura automată a metadatelor aparținând e-mail-urilor şi anexelor sale, aşa cum este schițat în modelul de metadate	D

Ref	Cerinţe	Testabil
	MoReq2.	
6.3.14.	SMAE trebuie să permită metadatele „data expedierii” şi „data primirii” să fie introduse manual. *Această prevedere are ca scop rezolvarea situațiilor în care datele deținute de mesajul e-mail nu sunt corespunzătoare setării activității (vezi introducerea la această secțiune pentru explicații asupra situațiilor posibile). O opțiune de configurare care să dezactiveze această facilitate va fi acceptabilă.*	D
6.3.15.	Un utilizator trebuie să aibă posibilitatea de a captura într-un SMAE, dintr-o singură operațiune, mai mult e-mail-uri selectate manual ca: ▪ un act sau ca ▪ un set de acte, unul pentru fiecare e-mail în funcție de opțiunea utilizatorului.	D
6.3.16.	SMAE ar trebui să fie capabil să identifice automat şi să captureze toate e-mail-urile înrudite cu un e-mail specificat de utilizator, într-o singură operațiune, capturându-le ca: ▪ un act sau ca ▪ un set de acte, unul pentru fiecare e-mail în funcție de opțiunea utilizatorului. *Secțiunea 3.6.4. „Câmpuri de identificare” din RFC 2822 descrie cum câmpurile opționale „Referitor la” [References] şi „ca răspuns la [In-Reply-To] din antetul SMTP pot fi folosite în asociere cu câmpul „Identificatorul mesajului” [Message ID] pentru a identifica mesajele de e-mail înrudite, uneori numite „firul discuției” (*thread*)*	D
6.3.17.	SMAE trebuie să permită unui utilizator care capturează un mesaj e-mail într-un format brevetat să îl salveze în multiple formate, inclusiv formate deschise. *Poate fi util pentru un SMAE să aplice criterii de salvare a e-mail-urilor bazate pe indicatoarele de termene de păstrare şi de dispoziție. Conținutul e-mail-urilor din dosare cu un termen de păstrare redus pot fi păstrate în format brevetat, dar cele cu termen de păstrare îndelungat ar putea fi salvate într-un format deschis.*	D
6.3.18.	Ori de câte ori câmpul de adresă capturat din antetul e-mail-ului apare în	D

Ref	Cerințe	Testabil
	metadatele unui act e-mail, SMAE trebuie să se asigure că el capturează atât opționalul „afişează nume” [display name] (dacă este prezent) al oricărei căsuțe poştale listate, cât şi „specificarea adresei” [address-spec]; de pildă, mai degrabă «Jan Schmidt» decât js97@xyz.int.	

6.4. Genuri de acte

Genul unui act descrie caracteristicile actelor care nu sunt (şi în mod obişnuit nu pot fi) definite în schema de clasificare. Acesta poate include anumite:

- atribute ale metadatelor
- cerințe de păstrare
- controale de acces
- felul documentelor (de ex. contract, CV, raport disciplinar)

Genul actului corespunde în mod obişnuit genului de document din care actul a rezultat.

Ref	Cerință	Testabil
6.4.1.	SMAE trebuie să accepte definirea şi întreținerea categoriilor de acte.	D
6.4.2.	Fiecare act din SMAE trebuie să aparțină unui singur gen de act.	D
6.4.3.	SMAE trebuie să încredințeze exclusiv rolului de administrator dreptul de definire şi întreținere a categoriilor de acte.	D
6.4.4.	SMAE trebuie să permită rolului de administrator să încredințeze crearea de acte dintr-un gen de acte specificat doar unui anumit grup de utilizatori, bazat pe nevoile lor de activitate.	D
6.4.5.	SMAE trebuie să permită rolului de administrator să definească un gen de act ca un gen de act standard, care să poată fi folosită de toți utilizatorii care au permisiunea de a captura acte.	

6.5. Scanarea şi producerea de imagini digitale

Când se planifică implementarea unui SMAE, este nevoie adesea să fie luate în considerare actele fizice sub formă de hârtie sau microforme.

Există două aspecte principale:

- acte existente care sunt păstrate pe hârtie sau microforme şi de care este nevoie pentru referințe în asociere cu actele electronice;
- documente pe hârtie care continuă să fie primite sau create de către organizație, dar pe

care organizația doreşte să le păstreze ca acte electronice în SMAE.

Această secțiune tratează scanarea (producerea imaginii) documentelor pe hârtie sau microforme, astfel încât ele să poată fi capturate într-un SMAE ca acte electronice. Sunt incluse câteva cerințe care se referă la detalii ale procesului de scanare.

Scanarea poate fi organizată în următoarele modalități:

- centralizată
- locală sau în grup de lucru
- externalizată sau subcontractată

sau în orice combinație. Aceste modalități sunt descrise pe scurt mai jos.

Scanarea centralizată este cea mai potrivită pentru captura de volum mare, utilizând în mod obişnuit echipament de scanare rapidă proiectat special pentru intrări masive, împreună cu operatori de scanare specializați.

Scanarea locală sau în grup de lucru are loc în apropierea utilizatorului destinatar şi este potrivită pentru activitatea cu volum mic, unde persoana care realizează scanarea are nevoie de o cunoaştere a activității, sau când este dictată de distribuția geografică a organizației. Se folosesc de obicei scanere de o capacitate şi viteză mici; pot fi uneori dispozitive multi-funcționale.

Scanarea externalizată sau subcontractată poate fi luată în considerare pentru un număr de motive legate de eficiența financiară:

- acolo unde există o mare cantitate de scanări ce trebuie efectuată ca o operațiune singulară
- acolo unde resursele umane suficiente nu există în cadrul organizației
- acolo unde spațiul de găzduire şi/sau echipamentul nu este disponibil în organizație
- acolo unde scanarea şi./sau depozitarea nu sunt condiționate de sediu

Restul acestei secțiuni stabileşte cerințele ce trebuie luate în considerare în furnizarea unei soluții integrate de SMAE şi scanare. Cerințele de aplică doar unde componentele de scanare sunt parte a SMAE. Multe din cerințe pot fi de asemenea interpretate pentru întrebuințare atunci când scanarea este externalizată.

Ref	Cerință	Testabil
6.5.1.	SMAE trebuie să fie capabil de integrare cu cel puțin o soluție de scanare. *Soluția de scanare furnizează interfața cu echipamentul de scanare şi permite operatorului să desfăşoare câteva procese relative la scanare, cum ar fi rotirea sau eliminarea zgomotului.*	D
6.5.2.	Componenta de scanare a SMAE ar trebui să accepte atât scanare monocromă, cât şi color. *Multe aplicații nu cer scanare color.*	D

Ref	Cerință	Testabil
6.5.3.	Componenta de scanare a SMAE trebuie să fie capabilă să salveze imaginile în formate standardizate, incluzând, dar nu limitându-se la: ▪ TIFF (vezi Specificația TIFF 6.0); ▪ JPEG (vezi ISO 15444, cerut doar dacă este acceptată culoarea) ▪ PDF/A (vezi ISO 19005).	D
6.5.4.	Componenta de scanare a SMAE trebuie să fie capabil de a salva imaginile la diferite rezoluții. *La modul ideal, caracteristica de scanare ar trebui să ofere un meniu de opțiuni, programabile pentru introducerea diferitelor categorii de documente.*	D
6.5.5.	Componenta de scanare a SMAE ar trebui să fie capabilă de a salva imaginile color sau pe scară de gri şi la diferite rezoluții.	D
6.5.6.	Componenta de scanare a SMAE trebuie să fie capabilă să întrebuințeze mărimile standardizate de hârtie, incluzând, dar nu limitându-se la: ▪ A4 ▪ A3 *Vezi ISO 216 pentru definirea A4 şi A3.*	D
6.5.7.	Componenta de scanare a SMAE ar trebui să conțină o funcționalitate OCR (recunoaştere optică a caracterelor). *Funcționalitatea OCR produce text dintr-o imagine scanată. Anumite genuri de OCR sunt uneori numite ICR (recunoaştere inteligentă a caracterelor). Pentru simplificare, MoReq2 le va denumi pe ambele OCR.*	D
6.5.8.	Acolo unde SMAE include o funcționalitate OCR, SMAE ar trebui să fie capabil să administreze imaginea scanată şi textul rezultat din OCR ca un singur act. *Altfel spus, textul ocerizat ar trebui să fie privit mai degrabă ca metadate ale actului decât un act propriu-zis.* *MoReq2 nu cere ca utilizatorii să fie capabili să vadă textul ocerizat, deoarece scopul său este să permită căutarea full-text (vezi cerința următoare).*	D
6.5.9.	Acolo unde SMAE include funcționalitatea OCR, ar trebui să permită căutarea în cadrul textului.	D

Ref	Cerință	Testabil
6.5.10.	Componenta de scanare a SMAE ar trebui sa fie capabilă de a recunoaşte şi captura documentele individuale într-un proces de scanare masivă. *MoReq2 nu specifică în ce mod s-ar putea realiza acest lucru. Soluțiile obişnuite se bazează pe recunoaşterea codurilor patch, a foilor patch, codurilor de bare sau inserturilor de foi albe.*	D
6.5.11.	Componenta de scanare SMAE trebuie să fie capabilă să transmită în mod automat unei cozi imaginile scanate, după scanare. *De exemplu, pentru indexare sau control de calitate.*	D
6.5.12.	SMAE ar trebui să includă o facilitate pentru inspectarea imaginilor scanate. *Aceasta poate include capacitatea de a accepta sau respinge imagini; şi, când ele sunt respinse, o cerere de rescanare.* *Inspectarea ar putea să fie realizată de un operator de scanner, de către un utilizator special însărcinat cu verificarea de calitate sau de către alt utilizator care desfăşoară activitatea de verificare a calității doar ca o parte a activității lor.*	D
6.5.13.	Componenta de scanare a SMAE-ului trebuie să permită rolului de administrator să seteze un nivel minim al parametrilor care descriu conținutul informațional al imaginii, în aşa fel încât orice imagine ai cărei parametrii sunt sub nivelul minim să fie eliminată ca reprezentând o pagina goală	D
6.5.14.	Componenta de scanare a SMAE -ului ar trebui să fie capabilă să stocheze parametrii de setare ai scannerului (cum ar fi față/față-verso; rezoluție; contrast; strălucire) pentru diferite categorii de documente.	D
	SMAE ar trebui să permită utilizatorilor să adnoteze imaginile	D
	Această caracteristică poate fi folosită pentru a nota probleme excepționale de scanare, sau pentru a face notițe (aşa cum adnotările manuale sunt folosite uneori în cazul documentației pe hârtie)	
6.5.15.	Dacă SMAE permite utilizatorilor să adnoteze imagini care sunt reținute ca acte, el trebuie să prevină alterarea şi înlăturarea acestor adnotări. *Aceasta este o cerință doar pentru acte; nu este cerință pentru alte imagini. Se urmărește să prevină modificarea actelor (sau să pară a fi modificate) temporar.*	D

Ref	Cerință	Testabil
6.5.16.	Dacă SMAE permite utilizatorilor să adnoteze imaginile care sunt reținute ca acte, el trebuie să stocheze împreună cu fiecare adnotare identitatea utilizatorului care face adnotarea şi ora şi data, de o manieră nemodificabilă. *Aceasta este o cerință doar pentru acte; nu este o cerință pentru alte imagini. Se urmărește asigurarea faptului că orice adnotare este cuvenită şi urmăribilă.*	D
6.5.17.	Componenta de scanare a SMAE ar trebui să înregistreze un jurnal pentru fiecare sesiune de scanare cu următoarele detalii: ▪ login-ul utilizatorului ▪ identificatorul stației de lucru ▪ ora şi durata ▪ identificatorul sesiunii ▪ identificatorul lotului ▪ numărul de documente (dacă e cazul) ▪ numărul de imagini scanate ▪ numărul de imagini după eliminarea paginilor albe (dacă paginile albe sunt eliminate automat)	D
6.5.18.	Componenta de scanare ar trebui să fie capabilă să captureze în mod automat metadatele relevante, atunci când se scanează formulare cu zone. *Un formular cu zone este unul care cuprinde arii definite în softul de scanare ca prezentând date care trebuie scanate. Informația din afara ariilor definite nu este scanată, astfel reducând mărimea imaginii şi reducând cerințele de stocare şi lățime de bandă.*	D
6.5.19.	Atunci când o componentă de scanare a SMAE include captura automată a metadatelor, ar trebui să fie capabilă să interpreteze aceste informații pentru clasificare automată. *Această componentă este în mod special utilă în cazul mediilor de lucru de caz, acolo unde actele pe hârtie în mod frecvent poartă identificatori de caz care conțin suficientă informație pentru a clasa un act — vezi secțiunea 10.5.*	D
6.5.20.	Un SMAE ar trebui să fie capabil de a importa masiv imagini scanate şi metadatele lor. *Vezi secțiunea 6.2 pentru mai multe referințe referitoare la importul în*	D

Ref	Cerință	Testabil
	grup.	
6.5.21.	ERMS-ul ar trebui să fie capabil să afişeze imagini în miniatură ale imaginilor scanate, pentru a ajuta navigația şi căutarea.	D
6.5.22.	ERMS-ul trebuie să permită utilizatorului să captureze imagini ca acte.	D

7. Trimiteri (referențieri)

Acest capitol aduce laolaltă cerințele pentru trimiteri între entități (clase, dosare, sub-dosare,volume şi acte) în cadrul unei scheme de clasificare. Secțiunea 7.1 prezintă cerințele pentru codurile de clasificare, iar cele pentru Identificatorii de sistem sunt prezentați în secțiunea 7.2.

Toate entitățile stocate în depozitele SMAE (clase, dosare, sub-dosare, volume, acte etc.) au nevoie de identificatori. Aceşti identificatori sunt necesari pentru:

- a permite software-urilor să proceseze entitățile;
- a permite utilizatorilor să regăsească, să se refere la şi să folosească entitățile;

MoReq2 foloseşte următoarea terminologie pentru a descrie aceşti identificatori:

- un identificator necesar pentru a fi utilizat de software este numit „identificator de sistem”. Acesta poate fi folosit în anumite cazuri atât de către utilizatori, cât şi de software.
- un identificator ierarhic aplicat entităților dintr-o ierarhie a unei scheme de clasificare şi destinată utilizatorilor este numit: cod de clasificare
- alți identificatori sunt denumiți în funcție de necesități, „identificatorul Programării de păstrare şi dispoziție”.

Diferența între Identificatorii de sistem şi Codurile de clasificare este ilustrată în următoarele 3 diagrame. Aceste diagrame vor fi de asemenea discutate mai târziu în capitol.

Figura 7.1 arată o parte a unei scheme de clasificare fictive, dar realistă. Ea arată câtva clase; fiecare clasă are un titlu de clasă (cum este cerut de 3.2.4).

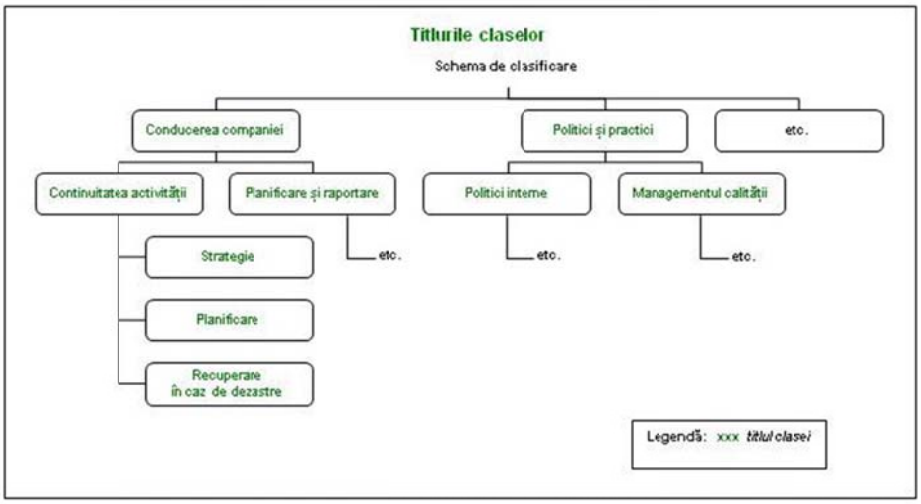


Figura 7.1

Fiecărei clase îi este alocat un indicativ de sistem, aşa cum este arătat în figura 7.2.

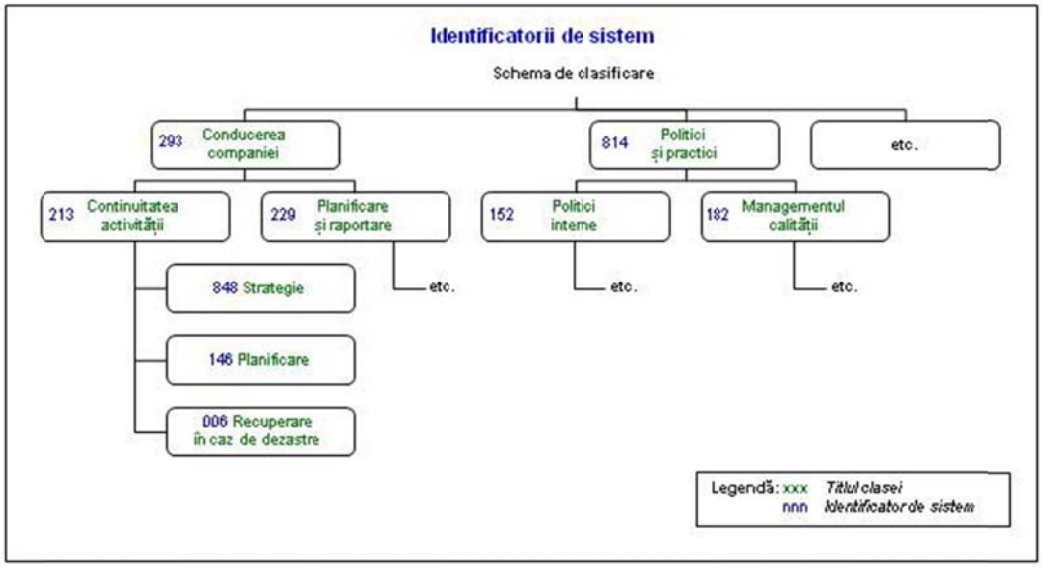


Figura 7.2

De observat că Identificatorii de sistem prezentați aici sunt de mici dimensiuni şi simpli, doar cu scop de ilustrare. În realitate, este posibil ca ei să aibă o dimensiune mai mare şi o structură mai complicată. Cu titlu de ilustrare, un exemplu al unui identificator de sistem bazat pe algoritmul „Identificator unic global” este 0c7220e3-5646-44c4-82b0-67832c1efa1c.

Şi claselor li se alocă Coduri de clasificare. Aşa cum este specificat în cerințele de mai jos, aceasta poate lua câtva forme; un exemplu este prezentat în figura 7.3.

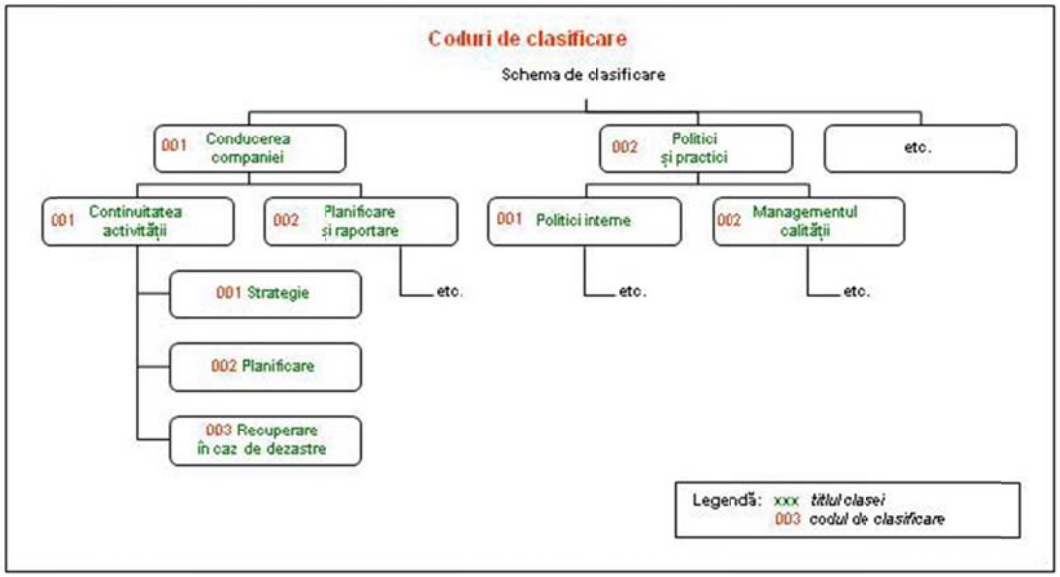


Figura 7.3

Şi aici, codurile de clasificare sunt prezentate ca relativ simple, pentru ilustrare.

Fiecare clasă are un cod de clasificare, ce poate fi combinat cu Codul de clasificare al clasei sale mamă, pentru a face un „cod de clasificare cu calificative complete”. Deci, de exemplu, codul de clasificare cu calificative complete al clasei *Recuperare în caz de dezastre* este 001-001-003. El este construit astfel:

- începe cu codul de clasificare al celui mai înalt dosar-mamă din ierarhie (001, fiind codul de clasificare al clasei *conducerea companiei*);
- adaugă codul de clasificare al următorului mamă, în jos din ierarhie (001, fiind codul de clasificare al clasei *continuitatea activității*), rezultând 001-001;
- repetă pasul anterior până este atinsă cea mai apropiată clasă-mamă(în acest exemplu, nu există repetări);
- adaugă codul de clasificare al clasei (003), care este codul de clasificare al clasei *recuperare în caz de dezastru*, rezultând astfel codul de clasificare cu calificative complete 001–001–003.

Coduri de clasificare sunt de asemenea alocate pentru acte şi componentele lor, pentru a permite să se facă în mod unic trimitere la ele.

Folosirea previzionată determină gradul de unicitate cerut. Identificatorii de sistem în general trebuie să fie unici cel puțin în cadrul unei instanțe SMAE sau al unui „nod de rețea” şi la nivelul întregii rețele, de preferat. Codurile de clasificare cu calificative complete trebuie să fie unice în cadrul unei scheme de clasificare, deşi, deoarece ele sunt construite ierarhic, codurile de clasificare pot fi unice doar în cadrul unui nod (de ex., o clasă sau sub-dosar) al ierarhiei.

Atunci când se cere un caracter unic în cadrul unei rețele, este de dorit ca identificatorii de sistem să fie bazați pe un standard recunoscut, care garantează caracterul unic la nivel global (adică unicitate în toate sistemele în orice moment). Aceasta este de asemenea de dorit pentru aplicațiile autonome, sau ne-cuprinse în rețele, astfel încât să permită posibile viitoare dezvoltări sau pentru activități de fuziune sau achiziție. Mai multe astfel de standarde au fot propuse, dar nici unul nu

are o poziție dominantă; MoReq2 prin urmare nu obligă la folosirea unui anume standard în acest scop.

7.1. Codurile de clasificare

Ref	Cerințe	Testabil
7.1.1.	Ori de câte ori o nouă apariție a oricărei entități din cele care urmează este creată în sau este capturată de către SMAE, acesta trebuie să asocieze un cod de clasificare pentru: ▪ clasă; ▪ dosar; ▪ sub-dosar; ▪ volum; ▪ act; ▪ componentă.	D
7.1.2.	SMAE trebuie să se asigure că toate codurile de clasificare cu calificative complete sunt unice în cadrul ierarhiei schemei de clasificare.	P
7.1.3.	SMAE trebuie să se asigure că toate codurile de clasificare şi codurile de clasificare cu calificative complete păstrează gradul cerut de unicitate indiferent de repoziționare (vezi cerința 3.4.1.).	D
7.1.4.	SMAE trebuie să fie capabil să stocheze codurile de clasificare ca elemente de metadate ale entităților la care se referă.	D
7.1.5.	SMAE trebuie să permită ca formatul codurilor de clasificare şi codurilor de clasificare cu calificative complete să fie precizat de rolul de administrator în momentul configurării sistemului. Ar trebui să permită următoarele caracteristici ale codurilor de clasificare să fie definite, pentru fiecare nivel al ierarhiei: ▪ numeric, alfabetic sau alfanumeric ▪ prezența sau absența zero-urilor inițiale ▪ lungimea minimă (în cazul zero-urilor inițiale) ▪ valoarea de pornite ▪ incrementarea	D
7.1.6.	Codurile de clasificare cu calificative complete trebuie să constea din concatenarea codurilor de clasificare separate printr-un caracter separator.	D

Ref	Cerințe	Testabil

7.1.7. SMAE ar trebui să permită caracterelor separatoare din Codurile de clasificare cu calificative complete să fie selectate din, cel puțin: D

„ ” (spațiu);

„–” (dash);

„/” (slash);

„.” (punct)

De exemplu, un cod de clasificare 01-001-003 (ca cel din introducerea de mai sus) ar putea fi prin urmare prezentat ca oricare din următoarele forme, în funcție de alegerile făcute pentru zerourile inițiale şi separatori la momentul confgurării:

1 001 003;

001-001-003;

1/1/3;

001.001.003.

Reamintind că cerința 3.2.7. permite prefixe globale şi extensii, acestea ar putea de asemenea să fie prezentate astfel:

corporate/1/1/3;

001.001.3.pt.

7.1.8. SMAE trebuie să permite unui rol de administrator să specifice, când o nouă clasă este creată, dacă entitatea-fiică va avea un cod de clasificare generat automat de către SMAE sau furnizat de utilizator/o aplicație externă. SMAE va trebui fie: P

- să genereze fiecare Cod de clasificare automat şi să împiedice utilizatorii să îl introducă manual şi, mai departe, să îl modifice (de pildă, un număr secvențial, ca în exemplul de mai sus)

sau

- să permită unui utilizator autorizat sau unei aplicații externe să furnizeze codul de clasificare, dar mai departe să împiedice modificarea lui.

Un exemplu pentru prima opțiune este dacă o nouă clasă intitulată „Managementul incidentelor” este adăugată sub clasa „Continuitatea afacerii” din exemplul prezentat în figura 7.3; în acest exemplu, va fi alocat codul de clasificare 004, aşa cum este prezentat în figura 7.4.

A doua opțiune este potrivită pentru setările de management al cazurilor.

Ref	Cerințe	Testabil
7.1.9.	Atunci când SMAE generează în mod automat un nou cod de clasificare (prima opțiune din 7.1.8), el trebuie să genereze următorul număr secvențial, luând în considerare: ▪ cel mai recent folosit cod de clasificare în acel punct al schemei de clasificare sau (pentru primul în acel punct) valoarea de început. ▪ valoarea de incrementare specificată, vezi 7.1.5. *Vezi figura 7.4. pentru un exemplu.*	D
7.1.10.	Atunci când acceptă un cod de clasificare de la un utilizator sau de la o aplicație externă, SMAE trebuie să îl valideze sub raportul unicității. sub nivelul-mamă.	D

7.2. Identificatorii de sistem

Ref	Cerințe	Testabil
7.2.1.	Ori de câte ori o nouă apariție următoarelor elemente este creată în SMAE, SMAE trebuie să o asocieze cu un identificator de sistem: ▪ schemă de clasificare ▪ clasă ▪ dosar ▪ sub-dosar ▪ volum ▪ act ▪ reeditare ▪ programarea de păstrare şi dispoziţie ▪ document	Y
7.2.2.	Un SMAE trebuie să se asigure că toți identificatorii de sistem sunt unici în cadrul ierarhiei schemei de clasificare şi în cadrul respectivei instanțe SMAE. *De observat că această cerință se extinde dincolo de amplasarea geografică acolo unde o schemă de clasificare dispersată a fost implementată şi dincolo de schemele de clasificare unde mai mult de o schemă de clasificare a fost implementată.*	N

Ref	Cerințe	Testabil
7.2.3.	SMAE trebuie să fie capabil să stocheze identificatorii de sistem ca elemente de metadate ale entităților la care se referă.	Y
7.2.4.	SMAE ar trebui să aloce identificatori de sistem care sunt unici la nivel global. *Unic la nivel global înseamnă că Identificatorii de sistem sunt alocați folosind un algoritm care garantează că nici un alt identificator de sistem nu poate avea aceeași valoare, indiferent de când a fost produs, sau de către care SMAE.* *Aceasta este de dorit pentru re-configurări, cum ar fi cele cauzate de reorganizări ale organizației, achiziții şi fuziuni etc. Dacă fiecărei entități nu îi este alocată un identificator de sistem de nivel global, este o mare probabilitate de apariție a dificultăților în timpul reconfigurării.*	N
7.2.5.	Un SMAE ar trebui să folosească algoritmul UUISD (aşa cum este specificat în ISO/IEC 9834–8 şi ITU-T Rec.X667) pentru a genera identificatori de sistem unici la nivel global. *Acest algoritm, la care în unele implementări se face referire sub forma GUID (Globally Unique ID), poate fi folosit pentru a garanta unicitatea.* *Alte abordări ale generației de identificatori unici pot fi folosite, incluzând Digital Object Identifier System (DOI®), schema Uniform Resource Name (URN) şi Archival Resource Key (ARK).*	P
7.2.6.	SMAE nu trebuie să ceară utilizatorilor să introducă sau să utilizeze identificatorii de sistem pentru nici o funcție a SMAE. *Această cerință este inclusă pentru că identificatorii de sistem la nivel global tind să fie lungi şi „neprietenoşi”. Totuşi, se poate accepta ca utilizatorilor să le fie permis să folosească identificatorii de sistem dacă ei aleg acest lucru.*	P

8. Căutare, regăsire şi prezentare

Acest capitol prezintă cerinţele pentru căutare şi regăsire în articolul 8.1. Cerinţele asociate cu prezentarea sunt împărţite în 3 secţiuni: secţiunea 8.2 prezintă cerinţele pentru afişare, secţiunea 8.3.se referă la imprimare şi secţiunea 8.4. tratează prezentarea actelor care nu pot fi imprimate.

O caracteristica de ansamblu a SMAE este posibilitatea ca un utilizator să regăsească dosare şi acte. Aceasta include căutarea lor, fie că detalii precise sunt cunoscute sau nu, şi prezentarea lor. Prezentarea înseamnă producerea unei reprezentări pe ecran („afişare”) sau imprimarea; ea poate de asemenea implica, acolo unde este cazul, redarea audio şi/sau video (vezi glosarul).

Accesarea dosarelor şi actelor, şi apoi vizualizarea lor, implică o gamă largă şi flexibilă de funcţii de căutare, regăsire şi prezentare, pentru a satisface cerinţele diferitelor tipuri de utilizatori. Deşi unele caracteristici de căutare pot fi gândite ca depăşind funcţiile clasice de administrare a actelor, funcţionalitatea cerută este descrisă aici în baza ideii că un SMAE fără posibilităţi de regăsire corespunzătoare este unul limitat ca valoare.

Toate caracteristicile şi funcţionalităţile din acest capitol trebuie să facă obiectul controlului de acces, aşa cum a fost descris în altă parte a acestei specificaţii, inclusiv controale de securitate. SMAE nu trebuie niciodată să prezinte informaţii vreunui utilizator care nu are dreptul să le acceseze. Pentru a evita complexitatea, acest fapt este subînţeles şi nu este repetat în fiecare cerinţă detaliată.

8.1. Căutare şi regăsire

Căutarea este procesul de identificare a actelor sau dosarelor prin intermediul unor parametrii definiţi de utilizator, cu scopul de a localiza, accesa şi regăsi acte, clase, dosare, sub-dosare, volume şi/sau metadatele lor.

Instrumentele de căutare şi navigare ale SMAE sunt folosite pentru a localiza metadate, clase, dosare, sub-dosare, volume sau acte. Acestea necesită o varietate de tehnici de căutare pentru a sprijini utilizatorii, de la (de pildă) sofisticatul utilizator „academic” până la cel „întâmplător” sau mai puţin „alfabetizat informatic”.

Ref	Cerinţă	Testabil
8.2.1.	Nicio funcţie de căutare sau de regăsire nu trebuie vreodată să dezvăluie unui utilizator vreo informaţie (metadate sau conţinut de act), acolo unde controale de acces şi securitate (secţiunile 4.1, respectiv 10.13) împiedică accesului acelui utilizator.	P

Ref	Cerinţă	Testabil
8.2.2.	SMAE trebuie să permită utilizatorilor să caute şi să regăsească: ▪ acte ▪ fiecare nivel de grupare al actelor (clasă, dosar, sub-dosar, volum) şi metadatele asociate lor, la orice nivel al schemei de clasificare.	D
8.2.3.	SMAE trebuie să permită utilizatorilor să precizeze orice combinaţie de elemente de metadate ca şi cuvinte cheie. *Instrumentul de căutare trebuie să fie capabil să caute după orice element de metadate, de pildă, Titlu.*	D
8.2.4.	SMAE trebuie să permită utilizatorilor să specifice dacă o căutare este destinată regăsirii de acte sau unui nivel precizat de grupare a actelor.	D
8.2.5.	Funcţia de căutare a SMAE ar trebui să fie identică pentru utilizatori, pentru toate tipurile de căutări specificate în cerinţa 8.2.2. *Cu alte cuvinte, utilizatorii ar trebui să vadă aceeaşi interfaţă, caracteristici şi opţiuni, fie pentru căutarea claselor, dosarelor, sub-dosarelor, volumelor sau a actelor (deşi detaliile prezentării rezultatelor pot varia în funcţie de ceea ce este cercetat).*	D
8.2.6.	SMAE trebuie să permită utilizatorilor să realizeze căutări în conţinutul actelor. *Aceasta include textul actelor care sunt implicit şi natural în format text, cum ar fi mesaje e-mail şi (acolo unde SMAE include funcţionalităţi OCR) actele care au fost convertite în format text prin ocerizare (vezi cerinţa 6.5.7).*	D
8.2.7.	SMAE trebuie să permită utilizarea de căutări pentru a localiza gruparea cu scop de declarare, ca parte a procesului de declarare. *Aceasta este o cerinţă pentru uşurinţa în folosire. Se solicită ca funcţionalitatea de căutare să fie disponibilă pentru utilizatorii care se află în proces de capturare a unuia sau mai multe acte; cu alte cuvinte, utilizatorii nu trebuie să fie obligaţi să abandoneze procesul de capturare pentru a iniţia o căutare.*	D
8.2.8.	SMAE trebuie să permită utilizatorilor să folosească orice combinaţie de elemente de metadate şi/sau conţinut textual al actelor ca și cuvinte cheie în timpul operaţiunii de căutare.	D

Ref	Cerinţă	Testabil
	De pildă, o căutare poate combina un anume autor cu o anumită secvenţă de text din cadrul actului.	
8.2.9.	SMAE ar trebui să ofere o funcţie de căutare care operează de o manieră integrată şi consecventă atât pentru acte, cât şi pentru metadate. *Această cerinţă presupune că interfaţa şi comportamentul ar trebui să fie aceleaşi pentru ambele tipuri de căutări.*	D
8.2.10.	SMAE trebuie să afişeze numărul total de itemi regăsiţi ca urmare a căutării şi să afişeze (sau să permită utilizatorului să ceară afişarea) unei liste de rezultate (*hit list*)	D
8.2.11.	SMAE ar trebui să permită utilizatorilor să perfecţioneze o căutare fără să fie nevoie să re-introducă criteriul de căutare. *Un utilizator ar trebui de pildă să aibă posibilitatea de a începe cu lista de regăsiri rezultată în urma unei căutări şi să realizeze o altă cercetare în cadrul acestei liste.*	D
8.2.12.	SMAE trebuie să permită rolului de administrator să configureze şi ulterior să modifice specificaţiile elementelor de metadate din căutarea de bază, incluzând: ▪ orice element al metadatelor aparţinând actului, volumului, sub-dosarului, dosarului şi clasei, şi ▪ opţional, text. *Această cerinţă se referă la fereastra de bază care apare atunci când este iniţiată o căutare; conţine în general, un set de câmpuri pentru elementele de metadate care sunt utilizate în mod obişnuit în căutări. Acest set cuprinde elementele de bază menţionate în cerinţă,*	D
8.2.13.	SMAE trebuie să furnizeze o funcţie de căutare care permite utilizarea operatorilor booleeni, respectiv: ▪ AND; ▪ OR; ▪ EXCLUSIVE OR; ▪ NOT; în orice combinaţie corectă pentru a combina un număr nelimitat de termeni de căutare.	P
8.2.14.	SMAE trebuie să permită utilizatorilor să caute pe baza cuvintelor cheie, acolo unde acele obiecte au cuvinte cheie.	D

Ref	Cerinţă	Testabil
8.2.15.	În cursul oricărei căutări bazate pe cuvinte-cheie, SMAE trebuie să permită utilizatorilor să selecteze cuvinte-cheie din vocabulare controlate (sau liste de termeni permişi) *Referindu-ne şi la cerinţa 8.2.7, această cerinţă se poate aplica în timpul procesului de captură sau în timpul oricărei alte căutări.*	D
8.2.16.	SMAE ar trebui să încorporeze utilizarea unui tezaur pentru a permite utilizatorilor să caute pe bază de concepte.	D
8.2.17.	Acolo unde un SMAE încorporează utilizarea unui tezaur pentru căutarea pe bază de concept, aceasta ar trebui să fie conform cu cel puţin unul din următoarele standarde: ▪ ISO 2788; ▪ ISO 5964 *Această cerinţă va permite regăsirea documentelor pe baza unui termen mai larg, mai îngust sau înrudit, aflat în conţinut sau în metadate. De pildă, o căutare pentru „servicii oftalmologice" ar putea regăsi „servicii de sănătate", „teste pentru ochi", oftalmologie".* *Primul standard se referă la un tezaur monolingv şi al doilea la un tezaur multilingv. (Vezi 3.2.13 şi 3.2.14).*	D
8.2.18.	Dacă un tezaur conform cu ISO 2788 sau ISO 5964 este integrat unui SMAE, acesta din urmă ar trebui să permită utilizatorului care efectuează o căutare pe bază de cuvinte cheie (sau alt element de metadate în legătură cu un tezaur) să folosească toate caracteristicile tezaurului, cum ar fi termeni hiperonimi, hiponimi sau asociaţi şi sinonime, ca o parte integrantă a procesului. *Cu alte cuvinte, dacă un utilizator caută un dosar, utilizatorul poate introduce un termen care nu este în schema vocabularului controlat, apoi foloseşte caracteristicile tezaurului pentru a identifica cuvântul cheie preferat potrivit. Un exemplu, dacă „bugete" este cuvântul-cheie preferat: în acest caz, utilizatorul ar putea introduce „estimări" şi apoi să fie ghidat către termenul hiperonomul „bugete" sau un utilizator ar putea introduce „acte contabile" şi să îi fie prezentată o listă cu termeni hiponimi, unul din ele fiind ,,bugete".* *Pentru uşurinţa în folosire, utilizatorii nu trebuie să fie obligaţi să părăsească interfaţa de căutare pentru a accesa tezaurul cu scopul de a căuta termenii de căutare înrudiţi. A se vedea introducere la secţiunea 11.8 pentru o explicaţie detaliată a expresiei: „ca o parte integrantă a procesului".*	D

Ref	Cerinţă	Testabil
8.2.19.	Acolo unde SMAE include utilizarea unui tezaur, SMAE trebuie să permită rolului de administrator să întreţină tezaurul. *Mentenanţa este necesară pentru introducerea de noi termeni şi termeni specifici activităţii.*	D
8.2.20.	SMAE trebuie să restricţioneze în favoarea rolurilor de administrator posibilitatea de a schimba cuvintele cheie asociate cu un dosar. *Această posibilitate este prevăzută doar pentru circumstanţe excepţionale, cum ar fi corectarea erorilor angajaţilor. Modificarea nepotrivită a cuvintelor-cheie poate compromite serios accesibilitatea actelor, chiar dacă este înregistrată în evidenţa de auditare şi ar trebui să fie evitată.*	D
8.2.21.	SMAE trebuie să ofere posibilităţi de căutare tip „potrivire parţială” sau „caracter universal”, care să permită adăugare de caractere înainte, după sau în ambele părţi ale caracterelor introduse de utilizator, atât pentru valorile metadatelor cât şi pentru conţinut. *De exemplu:* ▪ *căutarea termenului „proj” ar putea regăsi acte conţinând „project” şi „projection” şi „PROJA”;* ▪ *căutarea termenului „psycho*s” ar putea să regăsească acte conţinând „*psychosis”, „psychotics” şi „psychologists”; ▪ *căutarea termenului „*byte” ar putea să regăsească „*gigabyte”, „terabyte”. ▪ *căutarea termenului „organi?ation” ar putea să regăsească acte conţinând „*organisation” şi „organization”.	D
8.2.22.	SMAE ar trebui să ofere căutare de proximitate a cuvântului. *O căutare de proximitate găseşte termeni separaţi prin nu mai mult de un număr specificat de cuvinte, de exemplu:* ▪ *„International” şi „Organisation” separate prin nu mai mult de un cuvânt.*	D
8.2.23.	SMAE trebuie să permită utilizatorilor să limiteze aria de căutare a unei căutări la oricare grupare specificată de utilizator la momentul căutării	D
8.2.24.	SMAE trebuie să fie capabil să caute şi să regăsească un dosar, sub-dosar, sau volum electronic integral şi tot conţinutul şi toate metadatele contextuale şi să afişeze o listă a tuturor intrărilor (şi doar a acelora) din contextul acelor grupări, într-un singur proces de regăsire.	D

Ref	Cerinţă	Testabil
	Această cerinţă este necesară atunci când utilizatorul doreşte să copieze sau să imprime întregul conţinut al unui dosar pentru a-l lua la o întâlnire, sau să faciliteze munca într-un alt loc, sau pentru orice alt motiv.	
8.2.25.	SMAE trebuie să se comporte de o manieră identică atunci când efectuează căutări, indiferent dacă obiectul căutării este stocat pe dispozitive on-line near-line şi/sau offline, ținând totuși cont că mecanismul şi performanţa prezentării obiectelor electronice poate varia. *Această cerinţă se aplică doar când SMAE foloseşte stocarea near-line şi/sau offline pe lângă cea online.*	P
8.2.26.	SMAE ar trebui să permită utilizatorilor să salveze şi că refolosească termenii căutaţi.	D
8.2.27.	SMAE ar trebui să fie capabil să permită utilizatorilor să facă disponibili termenii de căutare salvaţi şi pentru alţi utilizatori.	D
8.2.28.	SMAE ar trebui să permită utilizatorilor să specifice intervalele de timp în cererea de căutare, de ex. datele din calendar sau numărul de zile.	D
8.2.29.	SMAE ar trebui să permită utilizarea ca termeni de căutare a intervalelor de timp specificate fie ca date (de ex. 24 dec. 2008–5 ian. 2009), fie în limbaj natural (de ex. „ultima săptămână”, „această lună”), permiţând folosirea a cel puţin următoarelor cuvinte şi/sau echivalentul lor în alte limbi: ▪ ultima ▪ această ▪ următoarea ▪ săptămână ▪ lună ▪ trimestru ▪ an ▪ numele zilelor săptămânii ▪ numele lunilor	D

Ref	Cerinţă	Testabil
8.2.30.	SMAE ar trebui să permită utilizatorilor sau rolurilor de administrator să configureze modul de afişare a rezultatelor căutării, incluzând: ▪ ordinea în care sunt prezentate rezultatele; ▪ numărul de regăsiri (*hits)* afişate pe ecran într-o singură vizualizare a căutării; ▪ numărul maxim de regăsiri dintr-o căutare ▪ ce elemente de metadate sunt afişate într-o listă cu rezultatele căutării	
8.2.31.	SMAE ar trebui să furnizeze ierarhia relevanţei, explicit sau predefinit, pentru aprecierea calităţii rezultatelor de căutare.	D
8.2.32.	Atunci când o listă de regăsiri conţine o re-editare a unui act electronic sau un act pentru care o re-editare există (vezi secţiunea 9.3), SMAE ar trebui să facă legătura între cele două, astfel încât regăsirea uneia dintre ele să indice şi existenţa celeilalte şi să permită regăsirea acesteia; supusă controlului de acces, cu păstrarea metadatelor separate pentru cei doi itemi.	D
8.2.33.	SMAE ar trebui să permită configurarea și a unui alt motor de căutare decât cel implicit. *O organizaţie poate dori să implementeze un motor de căutare diferit de cel livrat de SMAE, pentru compatibilitatea de sistem sau pentru alte motive.*	N

8.2. Prezentare: afişarea actelor

Un SMAE poate conţine acte în diferite formate. Utilizatorul solicită facilităţi generice de prezentare, care vor permite afişarea unei diversităţi de formate.

Ref	Cerinţă	Testabil
8.2.1.	Ori de câte ori un utilizator ajunge la un ecran care îi indică existenţa unei clase, dosar, sub-dosar, volum sau act, SMAE trebuie să fie capabil să prezinte conţinutul acestora şi/sau metadatele lor printr-o apăsare de mouse sau printr-o apăsare pe tastă. *Această cerinţă se aplică indiferent de cum primeşte utilizatorul imaginea — la navigare prin schema de clasificare, prin căutare, prin urmărea unui link sau prin orice altă cale — şi se presupune că utilizatorul are permisiunile necesare.*	D

Ref	Cerinţă	Testabil
	De exemplu: ▪ *un utilizator execută o căutare şi obţine o lista de rezultate prezentând câteva acte; pentru orice act, SMAE trebuie să fie capabil să prezinte conţinutul oricărui act din lista de rezultate, dacă utilizatorul realizează o apăsare de mouse sau apasă o tastă, şi trebuie de asemenea să fie capabil să prezinte în mod similar metadatele actelor.* ▪ *un utilizator navighează în schema de clasificare la o clasă care conţine dosare; SMAE trebuie să fie capabil să prezinte o listă a tuturor dosarelor cuprinse în clasa respectivă dacă utilizatorul apasă pe mouse sau apasă o tastă şi trebuie de asemenea să poată prezenta de o manieră similară metadatele clasei.* *Dacă un SMAE stochează actele într-un format de aplicaţie brevetată, se poate accepta ca prezentarea să fie realizată de o aplicaţie externă SMAE*	
8.2.2.	SMAE ar trebui să fie capabil să prezinte actele rezultate în urma unei cereri de căutare fără a încărca o aplicaţie asociată cu acel act. *De obicei, această cerinţă este îndeplinită prin integrarea într-un SMAE a unui program de vizualizare. Este frecvent de dorit, pentru a creşte viteza prezentării.*	D
8.2.3.	SMAE ar trebui să fie capabil să prezinte toate genurile de acte electronice specificate de organizaţie într-o manieră care păstrează informaţia din act (de pildă, toate caracteristicile prezentării vizuale şi de aşezare în pagină produse de aplicaţia care l-a generat) şi care prezintă împreună toate componentele unui act electronic. *Organizaţia trebuie să specifice aplicaţiile şi formatele cerute, şi în unele situaţii nivelurile acceptabile de fidelitate. În multe cazuri (de pildă, în aplicaţiile obişnuite de tip „office") fidelitatea necesară nu trebuie specificată detaliat; totuşi, o specificare riguroasă poate fi necesară pentru aplicaţiile care se bazează pe interpretări detaliate, cum ar fi actele incluzând imagini cu raze X de înaltă rezoluţie.*	N

8.3. Prezentare: imprimarea

Această secţiune se aplică doar pentru actele şi alte informaţii al căror conţinut poate fi imprimat de o manieră inteligibilă. Nu se aplică, de pildă, fişierelor audio sau video.

SMAE trebuie să furnizeze facilităţi de imprimare, pentru a permite tuturor utilizatorilor obţinerea de copii ale actelor care se pot imprima, a metadatelor acestora şi a oricăror alte informaţii administrative.

În toate cerinţele, termenul „imprimare” este înţeles ca incluzând caracteristici asociate în mod normal cu producerea de rapoarte, cum ar fi rapoarte pe mai multe pagini, numerotare file, antete datate, şi folosirea oricărei imprimante configurate. Transmiterea de capturi de ecran la o imprimantă nu este în mod normal considerată suficientă pentru aceste cerinţe.

Ref	Cerinţe	Testabil
8.3.1.	SMAE trebuie să fie capabil să imprime conţinutul actelor şi al elementelor specificate de metadate.	D
8.3.2.	SMAE trebuie să permită imprimarea tuturor metadatelor specificate pentru orice clasă, dosar, sub-dosar, volum sau act.	D
8.3.3.	SMAE trebuie să permită tuturor actelor dintr-o clasă, dosar, sub-dosar sau volum să fie imprimate într-o singură operaţiune.	D
8.3.4.	SMAE trebuie să permită utilizatorilor să specifice un subset de elemente de metadate (cum ar fi Titlu, Autor, Data creării) şi să imprime o listă rezumativă a acestor elemente pentru gruparea de acte selectată.	D
8.3.5.	SMAE ar trebui să permită unui rol de administrator să specifice în momentul configurării sistemului ca toate imprimările cuprinzând conţinutul actelor să fie însoţit de anumite elemente de metadate selectate implicit (de pildă, numărul de înregistrare, data, categoria de securitate). *Această cerinţă ar putea fi folosită, de pildă, pentru a se asigura că, ori de câte ori un act este imprimat, categoria de securitate este imprimat în acelaşi timp, ca o măsură de securitate.*	D
8.3.6.	SMAE ar trebui să permită utilizatorilor, în momentul imprimării, să modifice elementele implicite de metadate care sunt ataşate pentru imprimare.	D
8.3.7.	SMAE trebuie să permită utilizatorilor să imprime lista de rezultate (vezi secţiunea 8.1) dintr-o căutare.	D
8.3.8.	SMAE trebuie să permită rolului de administrator să imprime parametrii administrativi, parţial sau integral. *De exemplu, o listă a tuturor utilizatorilor deținând autorizații pentru acces la o anumită categorie de securitate sau a tuturor utilizatorilor dintr-un anumit grup de utilizatori.*	D
8.3.9.	SMAE trebuie să permită unui rol de administrator să imprime programarea de păstrare şi dispoziţie .	D

Ref	Cerinţe	Testabil
8.3.10.	Dacă un tezaur este integrat (vezi 8.2.16), SMAE ar trebui să permită rolurilor de administrator să imprime acest tezaur.	D
8.3.11.	SMAE trebuie să fie capabil să imprime o listă a fiecărui vocabular controlat (o listă cu toţi termenii acceptaţi). *Se acceptă imprimarea listei din aplicaţia de administrare a tezaurului, acolo unde acesta este integrat în SMAE.*	D
8.3.12.	SMAE ar trebui să poată exporta lista fiecărui vocabular controlat (lista tuturor termenilor acceptaţi).	D
8.3.13.	Acolo unde un vocabular controlat de cuvinte cheie ia forma unui tezaur conform cu ISO 2788 sau ISO 5964, SMAE ar trebui să fie capabil să imprime intrările din tezaur, prezentând toţi termenii şi relaţiile lor. *Imprimarea tezaurelor bazate pe standardele ISO ar trebui să fie compatibilă cu liniile directoare de reprezentare, existente în ISO 2788 şi ISO 5964.* *Se acceptă imprimarea acestora dintr-o aplicaţie separată de administrare a tezaurului, care este integrată cu SMAE.*	D
8.3.14.	SMAE trebuie să permită rolurilor autorizate să imprime schema de clasificare, atât în întregime, cât şi orice clasă selectată din schemă.	D
8.3.15.	Un utilizator care imprimă o schemă de clasificare (ca la 8.3.14) ar trebui să fie capabil să specifice conţinutul sau formatul produsului imprimării. *De exemplu, utilizatorul ar trebui să poată specifica elementele de metadate care urmează să fie imprimate şi de preferat să aleagă o reprezentare sub forma unei liste sau a unei alinieri indentate sau a unei reprezentări grafice.*	P
8.3.16.	SMAE trebuie să permită rolurilor de administrator să poată imprima o listă (uneori denumită inventar) a tuturor dosarelor sau a dosarelor clasificate într-o anumită clasă (şi a claselor subordonate).	D
8.3.17.	Un utilizator care imprimă o listă de dosare (ca la 8.3.16) ar trebui să fie capabil să specifice ordinea, conţinutul sau formatul listei. *De pildă, un utilizator ar trebui să fie capabil să sorteze în ordine crescătoare sau descrescătoare, după titlu sau cod şi de preferat pe baza oricărui alt atribut şi ar trebui sa fie capabil să specifice elementele de metadate care urmează să fie imprimate.*	D

Ref	Cerinţe	Testabil
8.3.18.	SMAE trebuie să permită rolurilor de administrator să imprime integral sau parţial evidenţa de auditare (vezi 4.2.1).	D
8.3.19.	SMAE trebuie să fie capabil să imprime formatele specificate de organizaţie. Imprimarea trebuie: ▪ să păstreze aşezarea în pagină produsă de aplicaţia generatoare. ▪ să include toate componentele imprimabile ale actului electronic. *Organizaţia trebuie să specifice formatele solicitate.*	D

8.4. Prezentare: alte situaţii

Această secţiune se aplică doar la actele şi la alte informaţii al căror conţinut nu poate fi imprimat de o manieră inteligibilă, cum ar fi fişierele audio şi video.

Ref	Cerință	Testabil
8.4.1.	SMAE trebuie să includă caracteristici pentru prezentarea şi generarea pe suportul corespunzător a actelor care nu pot fi imprimate. *Exemplele pot include audio, video şi unele web-site-uri. Organizaţia va trebui să specifice natura acestor acte.*	P

9. Funcții administrative

Acest capitol se referă la funcționalitățile de întreținere și de suport al sistemului, cerute de un SMAE.

- cerințele sunt listate în acest capitol pentru:
- administrare generală [secțiunea 9.1];
- raportări de sistem [secțiunea 9.2];
- Schimbarea, ștergerea și reeditarea actelor [secțiunea 9.3];

Caracteristici strâns legate sunt descrise în Capitolul 4, respectiv:

- permisiuni de acces în secțiunea 4.1;
- copie de siguranță și refacere în secțiunea 4.3.

Aceste facilități permit rolurilor de administrator să administreze schimbările la mulțimea utilizatorilor și la parametrii care reglează comportamentul sistemului. SMAE trebuie să furnizeze rolurilor de administrator posibilitatea de a administra evenimente cum ar fi mentenanța listei de utilizatori și, în mod esențial, permisiunile atribuite utilizatorilor, grupurilor și rolurilor. Sistemul trebuie de asemenea să furnizeze capacități de monitorizare pentru erori de sistem.

Unele dintre aceste facilități pot fi furnizate de către un SMDE asociat, un sistem de gestiune a bazelor de date sau de către alte aplicații

9.1 Administrare generală

Această secțiune include cerințe pentru administrarea parametrilor de sistem, administrarea și configurarea sistemului și administrarea utilizatorilor.

În organizațiile mari, funcționalitatea descrisă în această secțiune poate fi atribuită mai degrabă unei funcții operaționale decât unui administrator de aplicație. Cu toate acestea, în organizațiile mici, ea poate fi atribuită unui administrator.

Ref	Cerință	Testabil
9.1.1.	SMAE trebuie să permită rolurilor de administrator să regăsească, afișeze și re-configureze parametrii de sistem și setările făcute în momentul configurării sistemului.	D
9.1.2.	*Aceste setării includ, de exemplu, configurări ale drepturilor de acces și coduri de clasificare.*	

Ref	Cerință	Testabil
9.1.3.	SMAE trebuie să permită rolurilor de administrator să: ▪ aloce funcții utilizatorilor și rolurilor; ▪ aloce unuia sau mai multor utilizatori oricărui rol.	D
9.1.4.	SMAE trebuie să monitorizeze spațiul de stocare disponibil și să informeze rolurile de administrator când este nevoie de intervenție din cauză că spațiul de stocare este sub nivelul stabilit în momentul configurării sau din cauza unei alte condiții de eroare.	P
9.1.5.	*Se acceptă ca rolurile de administrator să fie înștiințate prin intermediul unei aplicații separate de administrare a sistemului.*	
9.1.6.	Acolo unde stocarea permite raportarea ratei de eroare, SMAE ar trebui să monitorizeze ratele de eroare produse pe suportul de stocare și să raporteze rolurilor de administrator orice suport sau dispozitiv a cărui rată de eroare depășește un parametru stabilit în momentul configurării sistemului sau la o dată ulterioară.	N
9.1.7.	*Această cerință se aplică în mod special pentru suportul optic.* *Se acceptă ca rolurile de administrator să fie înștiințate prin intermediul unei aplicații separate de administrare a sistemului.*	
9.1.8.	SMAE ar trebui să permită rolurilor de administrator să mute într-o manieră simplă utilizatorii între grupurile de utilizatori și roluri.	D
9.1.9.	*În special, ar trebui să fie posibil să mute un utilizator fără să fie nevoit să șteargă un utilizator dintr-un SMAE și să re-introducă detaliile utilizatorilor.*	

9.2 Raportare

Un sistem de raportare flexibil este o caracteristică importantă într-un SMAE. Se cere ca rolurile de administrator să administreze sistemul; ca urmare, administratorii să monitorizeze SMAE pentru a se asigura că este folosit în mod corespunzător.

Este necesar ca un SMAE să furnizeze un număr de rapoarte administrative, statistice sau ad-hoc, astfel încât rolul de administrator să poată monitoriza activitatea și starea sistemului. Acest sistem de raportări este cerut de-a lungul întregului sistem, incluzând:

- schema de clasificare
- dosare și acte
- activitatea utilizatorilor
- permisiuni de acces și securitate
- activități de dispoziție

SMAE trebuie să furnizeze un număr de rapoarte standard pe care rolurile de administratori să le poată configura și care ar trebui să fie flexibile pentru a permite ca rapoarte ad-hoc să fie produse

la cerere. La modul ideal, SMAE va include un sub-sistem flexibil de scriere a rapoartelor. Totuși, nu este potrivit să încercăm să prezentăm aici cerințele pentru un sub-sistem comprehensiv de scriere a rapoartelor astfel încât această secțiune oferă doar cerințe generale. Cantitatea și complexitatea rapoartelor va fi stabilită de caracteristicile organizaționale, incluzând mărimea, complexitatea și nivelurile de schimbare aduse schemei de clasificare, cantitatea și natura actelor, precum și mulțimea de utilizatori.

Ref	Cerință	Testabil
9.2.1.	SMAE trebuie să permită rolurilor de administratori să producă rapoarte periodice (zilnice, săptămânale, lunare, trimestriale) și să întocmească rapoarte ad-hoc.	D
9.2.2.	SMAE trebuie să includă caracteristici pentru imprimarea rapoartelor, vizualizarea lor pe ecran și stocarea lor în format electronic. *La fel ca în secțiunea 8.3, se presupune că termenul „imprimare" include caracteristici asociate în mod obișnuit cu producerea de rapoarte, cum ar fi rapoarte cu mai multe pagini, numerotare pagini, antete datate, antete și subsoluri de pagină configurabile și utilizarea oricărei imprimante configurate. Trimiterea spre imprimantă a unor simple imagini de pe ecran nu este, în mod obișnuit, considerată ca suficientă din perspectiva prezentelor cerințe.*	D
9.2.3.	Un utilizatori care vizualizează un raport generat de SMAE ar trebui să fie capabil să îl captureze ca act. *Această cerință ar putea fi folosită, de exemplu, pentru a stoca în siguranță rapoarte care atestă integritatea actelor.*	D
9.2.4.	SMAE ar trebui să permită ca perioadele de timp acoperite de un raport să fie configurate, fie ca un interval de timp (de pildă, 24/12/2008–5/1/208) sau ca un interval de timp specificat în limbaj natural (de pildă 8.2.29)	D
9.2.5.	SMAE trebuie să includă caracteristici pentru sortarea și selectarea informațiilor incluse în rapoarte. *De exemplu, utilizatorii ar trebui să poată specifica ce coloană a unui raport sub formă de coloane este folosită pentru a sorta conținutul raportului.*	D
9.2.6.	SMAE ar trebui să includă caracteristici pentru calcularea totalului sau de rezumare a informațiilor din raport.	D
9.2.7.	SMAE ar trebui să includă caracteristici pentru raportarea grafică. *De exemplu, rapoarte de tendință, prezentând schimbări în informațiile raportate de-a lungul timpului sau histograme.*	D
9.2.8.	SMAE ar trebui să permită să fie salvate cererile de rapoarte pentru o re-utilizare ulterioară.	D
9.2.9.	SMAE trebuie să permită ca rapoartele să fie exportate pentru utilizare în	D

Ref	Cerință	Testabil
	alte aplicații. *De exemplu, utilizatorii ar putea dori să lucreze cu conținutul unui raport folosind o aplicație cu foi de calcul tabelar. MoReq2 nu specifică formatul (formatele) care ar trebui folosite pentru asemenea exportări.*	
9.2.10.	SMAE trebuie să fie capabil să furnizeze rapoarte asupra numărului total și a localizării: ▪ dosarelor, sub-dosarelor și volumelor; ▪ actelor, sortate după formatul de fișier și versiune; ▪ dosare, sub-dosare și volume, sortate după restricțiile de acces și marcajele de securitate (acolo unde este cazul); ▪ dosare electronice, sub-dosare și volume, sortate după locul stocării; ▪ acte vitale	P
9.2.11.	SMAE trebuie să fie capabil să furnizeze rapoarte asupra: ▪ ratei de captură a actelor; ▪ ratei de regăsire a actelor; ▪ rata de creare a noilor clase și dosare.	D
9.2.12.	Dacă opțiunea de administrare a documentelor descrisă în secțiunea 10.3 este prezentă, SMAE trebuie să fie capabil să furnizeze rapoarte asupra: ▪ numărului total și localizarea documentelor; ▪ rata de captură/creare a documentelor; ▪ rata de regăsire a documentelor.	D
9.2.13.	SMAE ar trebui să permită rapoartelor descrise la 9.2.11 și la 9.2.12 să acopere orice combinație: ▪ de-a lungul întregului sistem sau pentru clasele selectate; ▪ pentru un grup de utilizatori specificat sau pentru utilizatori; ▪ pentru un interval specificat de date.	D
9.2.14.	SMAE ar trebui să fie capabil să furnizeze rapoarte asupra acțiunilor desfășurate asupra dosarelor și actelor sortate după utilizator, după stația de lucru și (acolo unde este cazul, din punct de vedere tehnic) după adresa de rețea.	P
9.2.15.	SMAE ar trebui să permită rapoartelor descrise la 9.2.11 să acopere un interval de timp precizat de câteva zile. *De exemplu, prezentând cifrele orare, să permită ca maximele și minimele activității să fie monitorizate.*	D

Ref	Cerință	Testabil
9.2.16.	SMAE trebuie să fie capabil să producă un raport care să listeze dosare, sub-dosare și volume, pentru schema de clasificare integrală sau parțială, structurat astfel încât să reflecte schema de clasificare.	D
9.2.17.	SMAE trebuie să fie capabil să furnizeze un raport asupra spațiului de stocare al sistemului, folosit și disponibil la un moment dat.	D
9.2.18.	SMAE trebuie să permită rolurilor de administrator să producă rapoarte despre evidența de auditare. Aceste rapoarte trebuie să includă, cel puțin, raportări bazate pe elemente selectate precum: ▪ clasă; ▪ dosar; ▪ sub-dosar; ▪ volum; ▪ act; ▪ utilizatori; ▪ perioadă de timp.	D
9.2.19.	SMAE ar trebui să permită rolurilor de administrator să interogheze și să producă rapoarte asupra evidenței de auditare bazate pe elemente selectate precum: ▪ categorii de securitate; ▪ grupuri de utilizatori; ▪ alte metadate.	D
9.2.20.	SMAE trebuie să fie capabil să raporteze rezultatul unui proces de dispoziție prin listarea claselor, dosarelor, sub-dosarelor, volumelor și actelor eliminate cu succes și orice nereușite produse.	D
9.2.21.	SMAE trebuie să fie capabil să raporteze rezultatul unui proces de export prin listarea claselor, dosarelor, sub-dosarelor, volumelor și actelor exportate cu succes și orice nereușite produse.	D
9.2.22.	SMAE trebuie să fie capabil să furnizeze rolurilor de administrator rapoarte privind activitatea de dispoziție, incluzând acțiunile de dispoziție care sunt scadente.	D
9.2.23.	SMAE ar trebui să permită rolurilor de administrator să restricționeze accesul utilizatorilor la rapoartele selectate.	D
9.2.24.	SMAE trebuie să fie capabil sa furnizeze rolurilor administrative un raport despre încercările de violare a accesului și a altor politici de securitate. *Această cerință se aplică doar când SMAE (și/sau sistemul de operare) este astfel configurat încât să permită ca existența unui item să fie vizibilă chiar dacă utilizatorului nu i se permite accesul la acesta. Cerința nu este*	D

Ref	Cerință	Testabil
	relevantă dacă SMAE este configurat să ascundă existența unui item care nu poate fi accesat.	
9.2.25.	Rolurile de administrator ar trebui să fie capabile să specifice frecvența raportărilor pentru programarea de păstrare şi dispoziţie , informațiile care se raportează și evidențierea excepțiilor, cum ar fi scadența dispoziției.	D
9.2.26.	SMAE ar trebui să furnizeze rapoarte cantitative asupra felurilor de acte care trebuie revizuite după un anumit termen.	D
9.2.27.	SMAE ar trebui să suporte instrumente de raportare și analiză pentru administrarea programărilor de păstrare și dispoziție, de către un rol de administrator, incluzând posibilitatea de a: ▪ lista toate programările de păstrare și dispoziție, sortate după motiv sau dată; ▪ lista toate entitățile cărora le este atribuită o anume programare de păstrare şi dispoziţie ; ▪ lista programările de păstrare şi dispoziţie care se aplică tuturor entităților dintr-o clasă; ▪ identifica, compara și revizui programările de păstrare şi dispoziţie (inclusiv conținutul lor) în cadrul schemei de clasificare. ▪ identifica contradicții de formă în programările de păstrare şi dispoziţie într-o schemă de clasificare.	D
9.2.28.	SMAE ar trebui să fie capabil să adune statistici ale deciziilor de revizuire dintr-o perioadă dată și să furnizeze rapoarte asupra acestei activități sub formă grafică sau de tabel.	D
9.2.29.	SMAE ar trebui să fie capabil să adune statistici ale suspendărilor și anulărilor de suspendări de dispoziție aplicate într-o perioadă dată și să furnizeze rapoarte asupra acestei activități sub formă grafică sau de tabel.	P
9.2.30.	SMAE trebuie să producă un raport care să detalieze orice nereușită înregistrată în timpul unui transfer, export, distrugere sau ștergere. Raportul trebuie să identifice orice act, grupare și metadate asociate destinate transferului care au generat erori de procesare și orice entitate care nu a fost transferată, exportată, distrusă sau ștearsă cu succes.	D
9.2.31.	SMAE trebuie să producă un raport care detaliază orice nereușită înregistrată în timpul unei importări. Raportul trebuie să identifice orice act, grupare sau metadate asociate, care sunt destinate importării, care au generat erori de procesare și orice entitate care nu a fost importată cu succes.	D
9.2.32.	SMAE ar trebui să sprijine procesul de importare, prin urmărirea și raportarea stării și progresului acestuia, incluzând procentajul îndeplinirii	D

Ref	Cerință	Testabil
	sarcinii și numărul de acte importat.	
9.2.33.	SMAE ar trebui să furnizeze posibilitatea de a sorta dosarele electronice selectate pentru transfer într-o listă ordonată, în conformitate cu elementele de metadate selectate de utilizator.	D
9.2.34.	SMAE ar trebui să furnizeze posibilitatea de a genera rapoarte definite de utilizator, pentru a descrie dosare și acte electronice care sunt exportate sau transferate.	D

9.3. Modificarea, ștergerea și reeditarea actelor

Un principiu de bază al activității de întocmire a actelor (*recordkeeping*) este că acestea nu pot, în mod normal, să fie modificate și (exceptând sfârșitul ciclului lor de viață în SMAE) dosarele, sub-dosarele, volumele și actele nu pot fi în mod normal distruse.

Această secțiune se referă la cerințele pentru situații excepționale, când este necesar ca un conținut al unui act declarat să fie amendat, sau un act să fie șters și înlocuit. În anumite situații, rolurile de administrator ar putea avena nevoie să „șteargă" acte pentru a putea corecta erori și a respecta cerințe legale. Un exemplu ar putea fi cel impus de legislația privind protecția datelor personale, deși sunt posibile și alte situații.

Acțiunea de ștergere poate avea două semnificații:

- distrugere
- păstrare, însoțită de o notificare în metadatele actului, precum că actul este considerat înlăturat de sub controlul administrării actelor.

În ambele cazuri, ștergerea trebuie să aibă un caracter excepțional, și în consecință posibilitatea de a șterge trebuie să fie sever controlată, pentru a putea proteja integritatea generală a actelor. În particular, informațiile despre ștergeri trebuie să fie stocate în evidența de auditare.

Dacă legislația sau reglementări impun cerințe diferite, de pildă legate de eliminarea datelor personale (vezi ISO 12037), acest aspect ar trebui tratat în Capitolul 0 referitor la aspectele naționale.

Rolurile de administrator pot avea nevoie, uneori, să facă publice sau să facă disponibile acte cuprinzând informații care sunt încă secrete, fără a divulga informațiile secrete. Aceste situații pot rezulta ca urmare a regulilor de protecție a datelor personale, considerații de securitate, riscuri comerciale etc. Din acest motiv, este necesar ca rolurile de administrator să poată masca informațiile secrete, fără a afecta actul în ansamblul său.

Procesul este denumit în continuare ca reeditare. Atunci când se desfășoară acest proiect, rezultatul este actul original (neschimbat) și o copie a actului care a fost mascată în anumite moduri (copia reeditată sau reeditarea actului original). SMAE stochează atât actul original, cât și **reeditarea**.

În principiu, redactarea se poate aplica la orice fel de act — text, imagine, audio, video etc. De remarcat că ștergerea și modificarea sunt de asemenea discutate în capitolul 5.

Ref	Cerințe	Testabil
9.3.1.	SMAE trebuie să permită o opțiune de configurare care împiedică orice act, odată capturat, să fie șters sau mutat de către orice rol, de administrator sau de utilizator; vezi de asemenea 9.3.3 *Această cerință nu afectează transferul sau distrugerea actelor conform cu programarea de păstrare şi dispoziţie , așa cum este descris la 5.3. Ea este destinată pentru mediile în care ștergerea actelor (așa cum a fost descrisă mai sus) este fie nu este necesară, fie nu este permisă. Alternativa la această opțiune este specificată la 9.3.2.*	D
9.3.2.	SMAE trebuie să permită o opțiune de configurare, ca o alternativă la 9.3.1, prin care „ștergerea" unui act să fie implementată ca distrugere a acelui act și prin care repoziționarea unui act să determine mutarea acelui act; vezi de asemenea și 9.3.4. *Această situație nu este privită ca o bună practică în managementul actelor. Este inclusă aici doar pentru situațiile în care sunt considerate inevitabile. În majoritatea situațiilor, opțiunea specificată la 9.3.1 ar trebui să fie aleasă. Această opțiune și opțiunea 9.3.1 sunt reciproc excluse.*	D
9.3.3.	Dacă opțiunea de la 9.3.1 este selectată, SMAE trebuie să se comporte astfel: ▪ dacă un rol de administrator „șterge" un act (în sensul lui 9.3.5), metadatele actului trebuie administrate în consecință și SMAE -ul trebuie să ascundă utilizatorilor conținutul și metadatele actului, ca și cum ar fi șterse, exceptând poate administratorilor autorizați în acest sens, iar SMAE trebuie să înregistreze acțiunea în evidența de auditare. ▪ dacă rolul de administrator mută un act (în sensul lui 3.4.1), SMAE trebuie să se comporte exact ca la fel ca în cazul unei ștergeri, dar cu adăugirea că o copie (sau un pointer, în funcție de metoda de stocare folosită) trebuie să fie inserat automat la noua poziție. *Se presupune că fie nici un rol de administrator nu va avea o asemenea autorizare, fie va fi un număr restrâns.*	D
9.3.4.	Dacă este selectată opțiunea 9.3.2, SMAE trebuie să se comporte astfel: ▪ dacă un rol de administrator șterge un act (în sensul lui 9.3.5) actul trebuie să fie șters, împreună cu metadatele sale, cu excepția metadatelor specificate ca făcând parte din urma de metadate al respectivului act (vezi 5.3.17]; și SMAE trebuie să înregistreze această acțiune în evidența de auditare. ▪ dacă rolul de administrator repoziționează un act (în sensul lui 3.4.1), SMAE trebuie să se comporte exact ca la fel ca în cazul unei ștergeri, dar cu adăugirea că o copie (sau un pointer, în	D

Ref	Cerințe	Testabil
	funcție de metoda de stocare folosită) trebuie să fie inserat automat la noua poziție.	
9.3.5.	SMAE trebuie să permită rolurilor de administrator să șteargă clase, dosare, sub-dosare, volume și acte, în afara procesului de dispoziție. *Această cerință este destinată a fi folosită doar în situații excepționale, cum este descris în această secțiune. Cerința trebuie citită împreună cu 9.3.1 și 9.3.2.*	D
9.3.6.	SMAE trebuie să permită rolurilor de utilizator să marcheze clase, dosare, sub-dosare, volume și acte ca fiind destinate ștergerii. *Rolul de administrator poate decide dacă va proceda la ștergere sau nu.*	D
9.3.7.	În cazul oricărei ștergeri, așa cum a fost definită mai sus, SMAE trebuie: ▪ să înregistreze ștergerea în evidența de auditare; ▪ să producă un raport pentru rolurile de administrator; ▪ să șteargă întregul conținut al unei clase, dosar, sub-dosar, volum atunci când este șters; ▪ să se asigure că nici un document nu este șters dacă această ștergere ar genera schimbări într-un alt act (de pildă, dacă un document este parte a două acte, unul din ele fiind șters); ▪ să evidențieze rolurilor administrative orice legături de la un alt dosar, sau de la act la dosar, sub-dosar sau volum care urmează să fie șterse, solicitând confirmarea înainte de efectuarea ștergerii. ▪ să mențină în orice moment integritatea metadatelor. *În acest context, formularea „să mențină integritatea metadatelor”înseamnă să se asigure că nici o metadată dintr-o entitate (clasă, act etc.) nu se referă la o entitate care nu mai există.*	D
9.3.8.	Rolurile de administrator trebuie să fie capabile să modifice orice element de metadată introdus de un utilizator. *Această funcționalitate este concepută pentru a permite rolurilor de utilizatori să corecteze erorile utilizatorilor, cum ar fi erori de scriere, și să întrețină accesurile pentru grupuri și utilizatori. Buna practică, în general, va cere ca utilizatorii să își corecteze erorile ori de câte ori este posibil; această cerință nu împiedică utilizatorii de a proceda astfel.*	D
9.3.9.	Informațiile despre toate schimbările aduse elementelor de metadate trebuie să fie stocate în evidența de auditare.	D
9.3.10.	SMAE trebuie să permită rolurilor de administrator să creeze una sau mai multe reeditări ale unui act, cu păstrarea formei originale a actului.	D

Ref	Cerințe	Testabil
	Poate fi necesar, în unele cazuri, să fie furnizate reeditări pentru mai multe părți, și pentru fiecare să fie reeditate alte porțiuni din act.	
9.3.11.	SMAE trebuie să permită înlăturarea sau ascunderea printr-o reeditare a informațiilor secrete, pentru toate formatele de acte specificate de organizație. *Dacă SMAE nu furnizează aceste facilități, el trebuie să permită altor aplicații să fie integrate și să procedeze astfel. Se acceptă ca SMAE să producă un act în alt format de fișier, astfel încât să permită reeditarea copiei, cu condiția ca acea copie să aibă o fidelitate suficientă.* *Este esențial ca, atunci când această caracteristică sau alte caracteristici de reeditare sunt folosite, nici una din informațiile eliminate sau ascunse să nu poată vreodată fi regăsite în reeditare, fie pe ecran, la imprimare, ascultare sau orice altă formă de prezentare. Aceasta cerință se aplică indiferent de modul de folosire al oricărei caracteristici de prezentare, cum ar fi rotirea, mărirea sau orice alt tip de manipulare, inclusiv deschiderea reeditării într-o altă aplicație.*	P
9.3.12.	Atunci când o reeditare este creată, SMAE trebuie în mod automat să stocheze crearea sa în metadatele reeditării și actului, inclusiv data, ora și creatorul.	D
9.3.13.	Atunci când o reeditare este creată, SMAE trebuie să solicite utilizatorului care o creează să introducă un motiv și trebuie să stocheze acel motiv în metadatele copiei reeditate și ale actului.	D
9.3.14.	În momentul creării unei reeditări, SMAE ar trebui în mod automat să declare reeditările drept acte, să le clasifice în aceeași grupare ca și actul original și să ceară creatorului să completeze: ▪ un motiv (vezi 9.3.13); ▪ categoria de securitate (dacă e cazul); ▪ opțional, o grupare în care reeditări să fie declarată.	P
9.3.15.	La crearea unei reeditări, SMAE ar trebui să permită copierea elementelor de metadate în reeditare.	D
9.3.16.	Cu respectarea drepturilor de acces, SMAE ar trebui să permită modificarea valorilor unor metadate selectate, de pildă titlul.	D
9.3.17.	SMAE ar trebui să stocheze o referință încrucișată către o reeditare în aceeași clasă, dosar, sub-dosar sau volum ca cea a actului original, chiar dacă clasa, dosarul, sub-dosarul sau volumul sunt închise. *Această cerință este suplimentară celei de a îndosaria o copie, conform 9.3.14, pentru a permite referențierea încrucișată chiar în același dosar, deoarece originalul și reeditarea pot fi separate printr-un mare număr de acte în dosar.*	D

Ref	Cerințe	Testabil
9.3.18.	Atunci când un act este regăsit, SMAE trebuie să prezinte, sau să permită utilizatorului să vadă, existența tuturor reeditărilor făcute după acel act, și, cu respectarea drepturilor de acces și de securitate, să le facă disponibile pentru regăsiri.	D
9.3.19.	Atunci când o reeditare este regăsită, SMAE trebuie să prezinte, sau să permită utilizatorului să vadă, existența actului original, și, cu respectarea drepturilor de acces și de securitate, să îl facă disponibil pentru regăsire.	D
9.3.20.	SMAE trebuie să stocheze în evidența de auditare orice modificare făcută ca rezultat al oricărei cerințe din această secțiune.	P

10. Module opționale

Acest capitol conține cerințe funcționale strâns legate de managementul actelor electronice. Sun acoperite cerințe menite să sprijine managementul actelor fizice (non-electronice), managementul documentelor, flux de lucru, semnătură electronică și alte funcționalități. Fiecare din secțiunile din acest capitol corespund unui modul opțional al Cadrului de Testare MoReq2. Aceste module sunt opționale în sensul că cerințele lor nu sunt o parte obligatorie a unui SMAE conform cu MoReq2.

Secțiunile în acest capitol prezintă cerințe pentru următoarele zone:

- managementul actelor fizice (secțiunea 10.1);
- dispoziția actelor fizice (secțiunea 10.2);
- managementul documentelor și activități în colaborare (secțiunea 10.3);
- flux de lucru (secțiunea 10.4);
- activități de caz (*casework*) (secțiunea 10.5);
- integrarea cu sisteme de conținut (*content system*) (secțiunea 10.6);
- semnături electronice (secțiunea 10.7);
- criptare (secțiunea 10.8);
- administrarea drepturilor digitale (secțiunea 10.9);
- sisteme dispersate (*distributed systems*) (secțiunea 10.10);
- activități offline și la distanță (secțiunea 10.11);
- integrarea faxurilor (secțiunea 10.12);
- niveluri de securitate (secretizare) (secțiunea 10.13);

Cerințele din acest capitol sunt pentru funcționalități opționale, care pot fi integrate cu un SMAE. Ele se adaugă cerințelor din restul MoReq2. Aceste cerințe se vor aplica doar dacă organizațiile au nevoie să implementeze funcționalitățile opționale.

Conformitatea cu cerințele din acest capitol nu este necesară pentru *conformitate MoReq2*. Prin urmare, cerințele obligatorii din acest capitol sunt obligatorii doar atunci când modulul opțional pe care îl descriu este inclus în testare.

În orice caz, cerințele sunt prezentate la un nivel general. Deoarece ele nu definesc funcțiile esențiale ale unui SMAE, aceste cerințe nu sunt exhaustive, ci doar oferă o orientare a activităților corespunzătoare.

10.1. Managementul actelor și dosarelor fizice (non-electronice)

În plus față de actele electronice, depozitele de arhivă ale unei organizații pot conține acte non-electronice. Acestea pot include acte pe hârtie sau acte pe alt suport analogic, de pildă microfișe sau benzi audio. Acestea pot include de asemenea acte electronice stocate pe suporturi portabile, cum ar fi CD, DVD sau benzi de computer.

Termenul de *acte fizice* este folosit în MoReq2 pentru a defini orice act care este păstrat într-un mediu din afara SMAE. Acesta include nu doar suport analogic, ci și suport digital care păstrează acte care nu sunt controlate la nivel individual de SMAE. De exemplu:

- un CD-ROM conținând 10 000 de imagini care nu sunt recunoscute individual de către SMAE ca acte, reprezintă un act fizic;
- un CD-ROM conținând 10 000 de imagini și aflate pe un disc sau tonomat conectat la SMAE și cu fiecare imagine recunoscută individual de către SMAE ca act nu este un act fizic — este un suport amovibil pe care actele electronice sunt stocate.

Aceste specificații nu tratează necesitățile din activitatea curentă de a administra și păstra actele fizice. Astfel de necesități pot sau nu să existe, conform cu mediul legislativ și de reglementare. Acolo unde există, este nevoie de măsuri pentru a păstra integritatea și accesibilitatea actelor fizice și electronice, luate ca un întreg. Aceste probleme ar trebui să fie tratate prin politicile organizaționale corespunzătoare.

SMAE trebuie să se poată adapta atât la referințele privitoare la actele fizice, cât și la cele electronice; și să administreze grupări formate atât din acte fizice, cât și din acte electronice. Clasele, dosarele, sub-dosarele și volumele pot conține toate orice combinație de acte fizice și electronice. Acest aspect este diferit de modelul entitate-relație din precedenta versiune MoReq2.

Actele electronice pot coexista cu actele electronice în câteva scenarii. Scenariile pot include:

- o clasă, dosar, sub-dosar sau volum care conține doar acte fizice. În acest caz, entitatea reprezentată în SMAE reprezintă un container fizic pentru acte, cum ar fi un dosar-plic.
- o clasă, dosar, sub-dosar sau volum care conține atât acte fizice, cât și electronice. Actele fizice sunt stocate fără vreun container relevant pentru managementul actelor — de exemplu, planuri inginerești păstrate laolaltă cu alte diferite planuri într-un sertar.

SMAE trebuie să furnizeze caracteristici pentru a permite containerelor fizice (ca în cazul primei opțiuni) să fie administrate.

Pentru a putea administra actele fizice, SMAE trebuie să poata să captureze și să administreze metadate despre acestea. Aceste metadate permit rolurilor de administrator și de utilizator (cu respectarea nivelurilor de acces) să localizeze, urmărească, regăsească, revizuiască și să elimine actele fizice și să aloce niveluri de acces în același fel ca și pentru actele electronice.

În mod similar, SMAE trebuie să poată captura și administra metadate despre containere.

Ref	Cerințe	Testabil
10.1.1.	SMAE trebuie să permită unui rol de administrator să identifice clasele, dosarele și volumele care există ca și containere fizice.	D

Ref	Cerințe	Testabil
10.1.2.	SMAE trebuie să permită rolurilor de administrator și de utilizator să introducă și să întrețină metadate despre clase, dosare, sub-dosare și volume care există ca și containere fizice, așa cum este specificat în modelul de metadate MoReq2.	D
10.1.3.	SMAE trebuie să permită rolurilor de utilizator să introducă și să întrețină informații despre actele fizice în clase, dosare, sub-dosare și volume, urmând aceleași reguli ca la capturarea actelor electronice.	D
10.1.4.	SMAE trebuie să permită claselor, dosarelor, sub-dosarelor și volumelor să conțină acte electronice și acte fizice la un loc, în orice combinație.	D
10.1.5.	SMAE trebuie să permită actelor fizice să fie administrate în același mod ca și actele electronice, inclusiv prin orice moștenire de metadate.	P
10.1.6.	Atunci când un utilizator parcurge, regăsește sau lucrează în alt mod cu o clasă, dosar, sub-dosar sau volum, SMAE ar trebui să indice prezența oricărui container fizic sau a actelor care se află în ele cu niște indicatori corespunzători. *Un utilizator are nevoie să determine cu ușurință dacă entități fizice există, cu scopul de a se asigura că toate actele sunt administrate de aceeași manieră. MoReq2 nu prescrie natura acestor indicatori.*	D
10.1.7.	SMAE trebuie să permită ca un set diferit de elemente de metadate să fie configurat de către un rol de administrator pentru clasele, dosarele, sub-dosarele, volumele și actele fizice, față de echivalentele electronice. Cu titlu de exemplu, metadatele pentru dosarele fizice ar putea include (dar nu se limitează la) metadatele adiționale pentru: ▪ informații asupra amplasării fizice; ▪ informații referitoare la formatul dosarului sau containerului fizic.	D
10.1.8.	La regăsirea oricărei clase, dosar, sub-dosar sau volum, SMAE trebuie să asigure regăsirea simultană, dintr-o singură operațiune, a metadatelor pentru entitățile fizice și cele pentru electronice asociate cu ele.	D
10.1.9.	SMAE ar trebui să accepte localizarea containerelor fizice și a actelor prin furnizarea de verificări la intrare și la ieșire pentru a înregistra poziția, custodele și data verificării de intrare/ieșire.	D
10.1.10.	SMAE ar trebui să permită ca utilizatorul să verifice la ieșire o grupare fizică sau un act la o anumită dată până la care el trebuie să fie returnat.	D
10.1.11.	SMAE ar trebui să raporteze unui utilizator specificat atunci când data precizată pentru înapoierea unei grupări fizice sau a unui act se apropie și când este depășită.	D
10.1.12.	SMAE ar trebui să permită unui utilizator abilitat să modifice data stabilită pentru înapoierea uneia sau mai multor grupări fizice sau acte, dintr-o	D

Ref	Cerințe	Testabil
	singură operațiune.	
10.1.13.	SMAE trebuie să se asigure că toate metadatele pentru grupări și acte sunt întotdeauna supuse acelorași condiții de acces care s-ar fi impus dacă ar fi fost doar electronice.	D
10.1.14.	SMAE ar trebui să furnizeze o funcție de localizare pentru a permite utilizatorilor să înregistreze informații despre poziția și mișcarea grupărilor și actelor fizice.	D
10.1.15.	Funcția de localizare a SMAE ar trebui să permită ca pozițiile entităților fizice să fie selectate din și validate cu o listă (cum ar fi o listă ascunsă). *Acolo unde SMAE nu acceptă o listă a pozițiilor, se acceptă și textul fără validare.*	D
10.1.16.	Funcția de localizare a SMAE trebuie să permită utilizatorilor să introducă verificările de intrare și ieșire pentru o entitate fizică. *Cu alte cuvinte, SMAE trebuie să furnizeze facilități pentru a înregistra dacă o entitate fizică este în poziția normală sau a fost verificată pentru ieșire de acolo.*	D
10.1.17.	Funcția de localizare a SMAE trebuie să înregistreze informații despre mișcarea unei entități fizice, care includ: ▪ identificator unic; ▪ poziția curentă; ▪ un număr (definit de către rolul de administrator) de poziții anterioare (numărul trebuie definit în momentul configurării sistemului); ▪ data mișcării din poziție; ▪ data primirii la poziție; ▪ utilizatorul responsabil cu deplasarea (acolo unde este cazul).	D
10.1.18.	SMAE trebuie să permită rolului de utilizator să vizualizeze, cu respectarea drepturilor de acces, poziția curentă a unei entități fizice verificată ca ieșită, custodele acesteia și data la care s-a produs verificarea de ieșire.	D
10.1.19.	SMAE trebuie să înregistreze în evidența de auditare toate activitățile de verificare de intrare/ieșire și data corespunzătoare.	D
10.1.20.	SMAE trebuie să înregistreze în evidența de auditare toate schimbările efectuate în valorile metadatelor entităților fizice. *De exemplu, elementul de metadată referitor la poziție.*	D
10.1.21.	SMAE ar trebui să accepte imprimarea și recunoașterea codurilor de bare, pentru dosare, sub-dosare, volume și acte; sau sisteme alternative de localizare cum ar fi tehnologia Identificare prin Frecvență Radio (RFID).	D

Ref	Cerințe	Testabil
	Această cerință permite SMAE să stabilească poziția și mișcările actelor fizice.	
10.1.22.	SMAE ar trebui să accepte imprimarea etichetelor pentru dosare, sub-dosare și volume fizice. *Această cerință permite producerea unei etichete care să conțină metadate esențiale, care poate fi apoi anexată entității fizice. Aceasta ar putea include (dar nu numai) metadate cum ar fi:* ▪ *titlu;* ▪ *identificator sistem;* ▪ *cod de clasificare;* ▪ *data deschiderii;* ▪ *categoria de securitate;* ▪ *amplasamentul normal de depozitare.*	D
10.1.23.	SMAE trebuie să se comporte într-o manieră identică atunci când operează cu acte electronice sau fizice în cadrul căutărilor, cu următoarele excepții: ▪ conținutul actelor fizice nu poate fi prezentat (în loc de conținut, SMAE va afișa metadatele de localizare, vezi mai jos); ▪ pot fi prezentate metadate diferite pentru actele fizice și cele electronice.	D
10.1.24.	SMAE ar trebui să poată notifica rolurilor de administrator orice evenimente în legătură cu programarea de păstrare şi dispoziţie aplicate actelor și grupările non-electronice, produse după momentul în care o refacere a fost executată. *Secțiunea 4.3 Copii de siguranță și revenire precizează cerințele pentru revenirea unui SMAE. Atunci când un sistem este folosit pentru managementul actelor non-electronice, se poate ivi o nepotrivire ca urmare a unei reveniri unde acțiunile de dispoziție s-au desfășurat asupra obiectelor fizice, dar aceasta nu este relevată de SMAE. Această cerință permite rolurilor de administrator să aplice acțiunile de remediere.*	D

10.2 Dispoziția actelor fizice

Ref	Cerințe	Testabil
10.2.1.	Atunci când un termen de păstrare pentru o programare de păstrare şi dispoziţie expiră, dacă programarea de păstrare şi dispoziţie se aplică oricărei entități fizice SMAE trebuie să notifice acest lucru rolului de administrator,.	Y

Ref	Cerințe	Testabil
10.2.2.	SMAE trebuie să alerteze un rol de administrator asupra existenței și poziției oricărei entități fizice asociate cu orice clasă, dosar, sub-dosar sau volum care trebuie să fie transferat, exportat sau distrus. *Aceasta se poate produce fie atunci când termenul de păstrare pentru o programare de păstrare şi dispoziţie expiră, fie când un transfer sau un export este inițiat.*	Y
10.2.3.	Ori de câte ori orice entitate fizică este exportată sau transferată, SMAE trebuie să exporte sau să transfere metadatele pentru acestea, în același fel în care procedează pentru metadatele entităților electronice.	Y
10.2.4.	La transferul, exportul sau distrugerea entităților fizice, SMAE trebuie să solicite unui rol de administrator să confirme transferul, exportul sau distrugerea fizică înainte de încheierea transferului, exportului sau distrugerii. *Prin această cerință în mod normal se va solicita rolului de administrator să introducă manual confirmarea că actele fizice au fost transferate sau distruse.*	Y

10.3 Managementul documentelor și activități în colaborare

Sistemele de Management al Documentelor Electronice — SMDE (EDMS) — sunt larg folosite în organizații pentrua permite evidența și managementul documentelor electronice. Multe funcții și facilități ale unui SMDE se suprapun peste cele ale unui SMAE. SMDE-urile includ în mod obișnuit indexarea documentelor, administrarea spațiului de stocare, evidența versiunilor, integrare strânsă cu aplicații tip desktop și instrumente de regăsire pentru a avea acces la documente. Unele SMAE furnizează capacități complete de SMDE, altele doar un subset. Reciproc, unele SMDE au încorporat funcții de bază din managementul actelor.

SMDE sunt adesea o parte a unei implementări de sisteme mai ample și cuprind instrumente pentru activitate în colaborare, pentru a permite unui număr mai mare de utilizatori să participe la proiectarea documentelor.

Activitatea în colaborare este de asemenea un element integrat în Sistemele de Management al Conținutului. Vezi secțiunea 10.6 pentru alte cerințe referitoare la aceste caracteristici.

Pentru lămurire, următorul tabel prezintă diferențe tipice între un SMDE și SMAE.

Un SMDE…	Un SMAE …
permite documentelor să fie modificate	protejează actele de modificări
permite documentelor să existe în câteva versiuni	permite existența unei singure versiuni finale a actului
poate permite ca responsabilii să își șteargă documentele	protejează actele împotriva ștergerii, cu excepția unor situații strict controlate
poate include o evidență de păstrare	trebuie să includă o evidență riguroasă de

	păstrare
poate include o structură de stocare a documentelor, care poate fi sub controlul utilizatorilor	trebuie să includă o structură riguroasă de ordonare a actelor (schema de clasificare), care este întreținută de rolul de administrator
este destinat în primul rând să sprijine folosirea zilnică a documentelor pentru activități în desfășurare	poate sprijini activitatea zilnică, dar este gândit în primul rând să furnizeze un depozit sigur pentru actele rezultate din activitate.

Continuarea acestei secțiuni stabilește cerințele care trebuie să fie luate în considerare la furnizarea unei soluții integrate SMDE/SMAE. Cerințele se aplică doar atunci când facilitățile SMDE sunt o parte a unui SMAE. O caracteristică centrală a acestor cerințe este conceptul că documentele pot fi stocate (adică, clasate) în aceleași clase și dosare ca și actele, deși acest lucru este opțional. Aceasta permite ca documentele-concept să fie îndosariate în aceleași grupări ca și versiunile finale, care vor fi acte.

De notat că termenul „document”este folosit aici cu semnificația precisă de a descrie informația sau obiectul care nu a fost declarat „act” într-un SMAE.

Ref	Cerința	Testabil
10.3.1.	SMAE ar trebui să poată administra acte și documente electronice în contextul aceleiași scheme de clasificare, folosind aceleași mecanisme de control al accesului. *Intenția acestei cerințe este să permită utilizatorilor să stocheze conceptele în grupările în care eventualul act va fi la rândul lui clasat. Această cerință este opțională.*	D
10.3.2.	Acolo unde SMAE administrează atât acte, cât și documente în cadrul aceleiași scheme de clasificare, trebuie să se indice cu claritate care elemente sunt acte și care documente. *MoReq2 nu precizează cum poate fi realizat acest lucru.*	D
10.3.3.	Acolo unde SMAE administrează atât documente, cât și acte în cadrul aceleiași scheme de clasificare, el trebuie să permită rolurilor de utilizator să desfășoare următoarele sarcini pentru orice clasă sau dosar specificat: ▪ să declare toate documentele ca „acte”; ▪ să șteargă toate documentele, păstrând doar actele; ▪ să șteargă toate documentele care sunt mai vechi decât o anumită perioadă.	D
10.3.4.	Acolo unde SMAE administrează atât documente, cât și acte în cadrul aceleiași scheme de clasificare, el trebuie să notifice unui rol de administrator dacă există documente într-o clasă sau într-un dosar care	D

Ref	Cerința	Testabil
	sunt exportate și să furnizeze ca opțiuni: ▪ să permită ca documentele să fie șterse; ▪ să le declare „acte”; ▪ să le exporte împreună cu actele.	
10.3.5.	Acolo unde un SMDE este parte a unui SMAE sau este strâns integrat cu un SMAE, SMDE trebuie să poată transfere în mod automat documentele electronice care sunt produse în cursul activității spre SMAE pentru capturare automată ca „acte”. *Această cerință este în mod special relevantă pentru scenariul dosarelor de caz; vezi de asemenea secțiunea 10.5.*	P
10.3.6.	SMAE trebuie să permită utilizatorilor : ▪ să captureze un document electronic și să îl declare „act” într-un singur proces; sau ▪ să captureze un document electronic, să îl stocheze și să încheie procesul de captură prin declararea lui ca act la un moment ulterior.	D
10.3.7.	SMAE trebuie să fie poată copia conținutul unui act electronic pentru a crea un document electronic nou și separat, fără a crea în mod automat și un nou act, în timp ce asigură păstrarea intactă a actului original. *De exemplu, un utilizator poate copia un act cu scopul de a trimite o copie la un destinatar care nu este un utilizator al SMAE. Această copie poate sau nu să fie declarată ca un nou act, în funcție de context.*	D
10.3.8.	SMAE trebuie să permită rolurilor de utilizatori să verifice la ieșire (vezi 10.3.11) orice document la care au drepturi de acces corespunzătoare.	D
10.3.9.	SMAE trebuie să permită rolurilor de utilizator să verifice la intrare orice document pe care l-au verificat la ieșire, oferind posibilitatea utilizatorului să îl verifice la intrare ca o nouă versiune sau nu (vezi 10.3.20).	D
10.3.10.	SMAE ar trebui să permită unui utilizator care verifică la intrare un document, să introducă, opțional, o explicație textuală a schimbărilor în timpul cât a fost verificat la ieșire.	D
10.3.11.	Atunci când un document este verificat la ieșire de un utilizator, SMAE trebuie să împiedice orice alt utilizator să îl verifice la ieșire sau să îl modifice (supusă cerinței 10.3.13).	D

Ref	Cerința	Testabil
	Atunci când un document este verificat la ieșire, doar utilizatorul care l-a verificat ca atare îl poate edita. *Această cerință se aplică doar documentelor. Prin însăși natura lui, un SMAE nu trebuie să permită nici unui act să fie verificat la ieșire sau să fie modificat.*	
10.3.12.	Atunci când un document este verificat la ieșire, dacă oricare alt utilizator încearcă să îl marcheze spre modificare, SMAE trebuie să nu permită utilizatorului să îl marcheze spre modificare a doua oară, să îl informeze pe utilizator că documentul este deja verificat la ieșire și trebuie fie: ▪ să prezinte identitatea utilizatorului care a verificat la ieșire; sau ▪ să ascundă identitatea utilizatorului care a verificat la ieșire, această opțiune fiind specificată în momentul configurării.	D
10.3.13.	SMAE trebuie să permită rolurilor de administrator să anuleze verificarea la ieșire a unui document. *Această cerință este destinată situațiilor în care un utilizator care a verificat la ieșire un document nu mai poate să îl verifice înapoi la intrare. Această situație poate apărea din mai multe motive, de pildă:* ▪ *utilizatorul a verificat documentul de pe un PC care s-a defectat sau a fost furat;* ▪ *documentul verificat s-a alterat (fișier corupt);* ▪ *utilizatorul a uitat să îl verifice la ieșire înaintea concediului*.	D
10.3.14.	Un utilizator nu trebuie să poată să verifice la intrare ca un același document o versiune a respectivului document, căruia i s-a anulat verificarea la ieșire (situația de la 10.3.13).	D
10.3.15.	Dacă se face o încercare de a închide o grupare din cadrul unui SMAE care conține și un document verificat la ieșire, această situație se raportează rolului de administrator ca o excepție.	D
10.3.16.	Utilizatorii trebuie să poată să captureze un document dintr-un EDMS.	D
10.3.17.	Utilizatorii trebuie să poată să treacă de o manieră simplă din și spre un SMAE pentru a declara un document ca act dintr-un SMDE. *Această cerință este în mod special importantă acolo unde SMAE/SMDE este folosit într-un spațiu obișnuit tip office*	N

Ref	Cerința	Testabil
10.3.18.	Acolo unde sunt versiuni multiple ale unui document, SMAE trebuie să poata să captureze documentele ca acte în toate modalitățile descrise mai jos, cu una dintre ele selectată ca opțiune predefinită în momentul configurării și cu utilizatorul abilitat să selecteze una dintre ele în timpul capturării: ▪ cea mai recentă versiune; ▪ o versiune care este specificată de utilizator; ▪ toate versiunile stocate, care să fie tratate ca un singur act; ▪ toate versiunile stocate, care să fie tratate ca acte separate, dar legate între ele.	D
10.3.19.	SMAE trebuie să mențină un număr de versiune pentru fiecare document și trebuie să îl facă ușor vizibil atunci când documentul este regăsit sau când este căutat.	D
10.3.20.	SMAE trebuie să crească în mod automat numărul versiunii documentului atunci când un document este verificat la intrare ca o nouă versiune.	D
10.3.21.	SMAE ar trebui să permită ca schema de numerotare a versiunii să fie definită în momentul configurării, permițând cel puțin următoarele opțiuni: ▪ numerotarea versiunilor în secvență simplă, adică numere de forma: 1, 2, 3; ▪ numerotarea versiunilor majoră și minoră, adică numerotare de forma x.y, unde x este versiunea majoră și y este versiunea minoră, iar versiunea minoră se resetează automat la 0 atunci când versiunea majoră primește următorul număr. *Alte scheme de numerotare sunt acceptate.*	D
10.3.22.	SMAE trebuie să permită ca maniera de stocare a versiunilor de documente să fie configurabilă de către un rol de administrator, în momentul configurării sistemului sau ulterior, la nivel de clasă sau de dosar în cadrul schemei de clasificare, având cel puțin următoarele opțiuni implicite pentru fiecare clasă și dosar: ▪ toate versiunile tuturor documentelor sunt stocate în clasă sau în dosar; ▪ doar cea mai recentă versiune (acolo unde rolul de administrator are posibilitatea de a specifica versiunile majore și minore) ale fiecărui document este stocată în clasă sau în dosar; ▪ un număr de versiuni ale fiecărui document este stocat în clasă sau în dosar, numărul fiind specificat de către rolul de	D

Ref	Cerința	Testabil
	administrator. *Această cerință este introdusă pentru a permite controlului versiunilor să fie folosite acolo unde un istoric al dezvoltării documentului este necesar. Acolo unde un istoric nu este necesar, numărul versiunilor stocate — și astfel, stocarea cerută — poate fi redus.*	
10.3.23.	SMAE ar trebui să permită utilizatorilor care stochează documente să ignore valoarea predefinită pentru versiunile (așa cum a fost definit la 10.3.22) care să fie stocate pentru respectivul document. *De pildă, momentul creării și autorul documentului, de asemenea metadatele identificabile din câmpuri structurate din documente, dacă acestea există, cum ar fi data și subiectul.*	D
10.3.24.	SMAE trebuie să permită unui utilizator să introducă valori de metadate pentru un act la momentul capturării.	D
10.3.25.	SMAE trebuie să se asigure că orice metadată care este capturată este administrată conform modelului de metadate MoReq2.	D
10.3.26.	SMAE ar trebui să permită unui utilizator autorizat să echivaleze elementele de metadate ale SMDE cu câmpurile de metadate corespunzătoare ale SMAE.	N
10.3.27.	Acolo unde există un conflict între metadatele SMAE și cele ale sistemului care a generat documentul, SMAE trebuie să avertizeze utilizatorul. *Această situație se poate produce atunci când SMAE nu are control asupra elementelor de metadate din document.*	D
10.3.28.	SMAE ar trebui să poată integra noile versiuni de SMDE sau sisteme pe măsură ce acestea sunt implementate de organizație. *MoReq2 nu specifică modul în care se poate produce acest lucru. Organizațiile ar trebui să ia în considerare specificarea acestei opțiuni de o manieră mai detaliată.*	N
10.3.29.	SMAE trebuie să poată controla versiunile, adică să poată administra diferite versiuni ale unui document electronic ca pe o singură entitate. *Această cerință sprijină procesul de creare de concepte ale unui document și permite activități în colaborare.*	D
10.3.30.	SMAE ar trebui să poată să îi limiteze pe utilizatori să vizualizeze: ▪ doar cea mai recentă versiune a unui document;	D

Ref	Cerința	Testabil
	▪ anumite versiuni selectate ale unui document; ▪ toate versiunile unui document; ▪ versiunile care au fost capturate sau înregistrate ca acte, opțiunea fiind făcută în momentul configurării sistemului sau la un moment ulterior, de către rolul de administrator.	
10.3.31.	SMAE ar trebui să permită utilizatorilor să aibă un spațiu de lucru „personal” pentru documente. *Acesta poate fi folosit de utilizatori pentru a stoca documente personale care nu sunt prevăzute a fi capturate ca acte, de pildă concepte preliminare care nu sunt corespunzătoare pentru a fi difuzate în cadrul organizației, sau alte documente. Folosirea acestui spațiu de lucru ar trebui să fie opțională (adică, ar trebui să fie posibil să se configureze SMAE astfel încât acesta să nu fie disponibil).*	D
10.3.32.	Acolo unde SMAE include un spațiu de lucru personal, un rol de administrator trebuie să poata să limiteze mărimea acestuia la nivel de utilizator.	D
10.3.33.	Acolo unde un SMAE include un spațiu de lucru personal, accesul la acesta trebuie să fie restricționat la posesorul acestuia.	D

10.4 Fluxul de lucru

Coaliția pentru Managementul Fluxului de Lucru (The Workflow Management Coalition, WfMC) — o asociație internațională pentru dezvoltarea de standarde referitoare la fluxul de lucru — definește fluxul de lucru drept „o automatizare a proceselor de activitate, în întregime sau în parte, în timpul căreia documentele, informațiile sau sarcinile sunt trecute de la un participant la altul pentru acțiune, în conformitate cu un set de reguli procedurale”. În această definiție, un „participant” poate fi un utilizator, un grup de lucru (de pildă, o echipă) sau o aplicație informatică.

Cerințele din această secțiune acoperă atât funcțiile de circulație de bază, așa cum sunt descrise în 6.3.35, cât și opțiuni sofisticate de flux cum ar fi gestionarea tranzacțiilor de mare volum cu excepții și rapoarte asupra performanței sistemului și a indivizilor. Cea de-a doua parte poate fi furnizată prin integrarea cu SMAE a unui produs de flux al unui terț.

Tehnologiile de flux transferă obiectele electronice între participanți sub controlul automatizat al unui program. În contextul unui SMAE, fluxul este folosit pentru a muta dosarele electronice și/sau documentele și actele între utilizatori, departamente și aplicații. El este folosit în mod obișnuit pentru:

- administrarea proceselor esențiale cum ar fi procedurile de înregistrare și dispoziție a dosarelor sau actelor;
- marcarea și aprobarea actelor anterior înregistrării;

- dirijarea dosarelor sau actelor într-o manieră controlată de la utilizator la utilizator pentru acțiuni specifice, de pildă marcarea documentelor, aprobarea de noi versiuni.
- notificarea utilizatorilor despre disponibilitatea actelor;
- distribuirea actelor;
- managementul actelor prin procese de activități de caz.

Ref	Cerințe	Testabil
10.4.1.	SMAE trebuie să permită fluxuri care constau dintr-un număr de pași procedurali, fiecare pas fiind (de pildă) mișcarea unui document, act sau dosar de la un participant la altul pentru acțiune sau decizie.	D
10.4.2.	SMAE trebuie să recunoască drept „participanți” atât utilizatori, cât și grupuri de lucru.	D
10.4.3.	Acolo unde participantul este un grup de lucru, caracteristica de flux a SMAE ar trebui să includă o opțiune pentru a distribui elementele sosite către membrii grupului prin rotație sau pe baza îndeplinirii de către membrii a sarcinilor curente, pentru a echilibra încărcarea membrilor echipei.	D
10.4.4.	SMAE trebuie să permită ca rolurile de administrator să definească fluxuri pre-programate.	D
10.4.5.	SMAE trebuie să permită rolurilor de administrator să salveze fluxurile pentru o folosire ulterioară. *Această cerință presupune ca fiecărui flux salvat să i se atribuie un identificator unic.*	D
10.4.6.	SMAE ar trebui să permită rolurilor de administrator care stochează fluxul să îi atribuie un titlu unic, sub formă text.	D
10.4.7.	SMAE trebuie să restricționeze în favoarea rolurilor de administrator sau utilizatorilor autorizați modificarea fluxurilor pre-programate.	D
10.4.8.	Ori de câte ori un rol de administrator modifică și stochează un flux, SMAE ar trebui să stocheze o copie a fluxului înainte de modificare sub forma unui act și ar trebui în mod automat să atribuie un nou număr de versiune pentru fluxul modificat, cu metadate care să specifice intervalul de data/timp în care a fost folosit.	D
10.4.9.	SMAE nu trebuie să limiteze numărul de fluxuri care pot fi definite și stocate.	P
10.4.10.	SMAE trebuie să înregistreze toate creațiile și schimbările fluxurilor pre-programate în evidența de auditare.	D

Ref	Cerințe	Testabil
10.4.11.	SMAE ar trebui să permită rolurilor de utilizatori să definească, să folosească și să salveze imediat fluxuri nou, definite de utilizator (uneori numite fluxuri ad-hoc).	D
10.4.12.	SMAE ar trebui să includă o interfață grafică pentru a permite rolurilor de administrator și de utilizator să definească, să întrețină și să editeze fluxuri.	D
10.4.13.	SMAE ar trebui să sprijine procesele de dispoziție, revizuire și de export/transfer, prin urmărirea și raportarea: ▪ progresului/stării revizuirii, cum ar fi așteptarea sau progresul, detaliile revizuirii și data; ▪ acte așteptând dispoziția ca rezultat al revizuirii deciziei; ▪ progresul procesului de transfer.	D
10.4.14.	SMAE trebuie să notifice unui rol de administrator dacă un act sau un dosar dintr-un flux este programat pentru revizuire sau dispoziție	D
10.4.15.	SMAE trebuie să se asigure că toate actele și dosarele își păstrează toate legăturile în cadrul unui proces de flux.	P
10.4.16.	SMAE ar trebui să administreze dosarele și actele în „cozi”, care pot fi examinate și controlate de rolurile de administrator.	D
10.4.17.	SMAE trebuie să permită rolurilor de utilizatori sa inițieze și să folosească fluxuri definite de rolurile de administrator.	D
10.4.18.	SMAE trebuie să permită utilizatorilor să monitorizeze progresul unui flux pe care l-au inițiat și la care participă.	D
10.4.19.	SMAE ar trebui să permită declararea automată a unui document să fie pas într-un flux.	D
10.4.20.	SMAE ar trebui să nu limiteze numărul de pași în fiecare flux.	P
10.4.21.	SMAE ar trebui să poată stabili priorități în cadrul cozii.	D
10.4.22.	SMAE ar trebui să includă prelucrarea întâlnirilor. *Această cerință presupune ca fluxul să se oprească pentru a aștepta sosirea unui act sau document electronic asociat. Atunci când elementul așteptat este primit, fluxul repornește în mod automat.*	D
10.4.23.	SMAE trebuie să permită definirea de roluri de flux distincte pentru diferiți utilizatori.	D

Ref	Cerințe	Testabil
	Exemple de astfel de roluri includ: ▪ *rol de administrator de flux (având aprobarea de a re-atribui sarcini și acțiuni către alt utilizator sau grup de lucru);* ▪ *rol de supraveghetor (având aprobarea de a stabili un flux pentru gestionarea excepțiilor în cazuri specifice);* ▪ *utilizatori sau grupuri de lucru pentru flux normal*.	
10.4.24.	SMAE ar trebui să permită rolului de administrator să definească numărul axim de pași dintr-un flux în momentul configurării.	D
10.4.25.	SMAE ar trebui să permită rolurilor de administrator care definesc un flux să asocieze limite de timp cu pași individuali și să raporteze unui utilizator nominalizat sau rolului de administrator acele elemente care sunt depășite conform acestor limite.	D
10.4.26.	SMAE ar trebui să permită rolului de administrator care definește un flux să aleagă dintr-o listă predefinită ce acțiuni vor trebui efectuate de participanții la flux.	D
10.4.27.	SMAE ar trebui să permită rolului de administrator care definește un flux să aleagă participanții: ▪ după nume ▪ după roluri ▪ după diviziunile organizației	D
10.4.28.	Rolurile de administrator ar trebui să poată aloca aprobări utilizatorilor individuali, astfel încât aceștia să poată reatribui sarcini/acțiuni într-un flux către alt utilizator sau grup. *Un utilizator ar putea dori să trimită un dosar sau un act către alt utilizator datorită conținutului actului, datorită faptului că utilizatorul destinat este în concediu sau pentru alte motive.*	D
10.4.29.	SMAE ar trebui să permită participanților să vizualizeze cozile de lucrări care le sunt adresate și ar trebui fie: ▪ să permită participanților să selecteze elementele pentru a acționa; sau ▪ să aducă elementele în atenție pe principul primul intrat-primul ieșit; Opțiunea trebuie să fie specificată atunci când este proiectat fluxul.	D

Ref	Cerințe	Testabil
10.4.30.	SMAE ar trebui să furnizeze fluxuri condiționate care depind de răspunsul utilizatorului sau de datele din sistem, pentru a decide sensul fluxului.	D
10.4.31.	SMAE ar trebui să permită utilizatorilor să suspende temporar un flux cu scopul de a putea desfășura alte activități și să îl continue mai târziu (inclusiv după de-logarea din sistem).	D
10.4.32.	SMAE trebuie să notifice unui utilizator participant atunci când un dosar sau acte au fost primite în atenția sa în mapa electronică (*tray*). *MoReq2 nu specifică dacă această „mapă”este în mapa contului de e-mail a participantului sau diferită de aceasta.*	D
10.4.33.	SMAE ar trebui să accepte urmărirea dosarelor și actelor prin opțiunea de furnizare viitoare de atenționări (numită adesea și memento („tickler”)) care permite unui utilizator să ceară o reamintire de acces la un dosar sau un act la o dată viitoare.	D
10.4.34.	SMAE trebuie să furnizeze un mecanism care să permită utilizatorilor să notifice altor utilizatori despre actele ce necesită atenția lor. *Acest mecanism poate utiliza un sistem de e-mail existent sau un sistem de mesagerie autonom sau patentat.*	D
10.4.35.	SMAE ar trebui să includă capacitatea de a declanșa în mod automat o instanță o a unui flux specificat atunci când un act de un gen anume specificat este primit. *De pildă, un flux pentru cereri de împrumut poate fi declanșat automat la primirea unui act cu genul de act „formular de cerere pentru împrumut”.*	D
10.4.36.	SMAE ar trebui să permită primirea, în dosarele specificate, a actelor sau documentelor electronice pentru a declanșa în mod automat fluxurile (fluxul fiind decis de genul de document sau de altă valoare de metadată).	D
10.4.37.	SMAE trebuie să furnizeze opțiuni detaliate de raportare pentru a permite utilizatorilor autorizați și rolurilor administrative să monitorizeze cantități, performanțe și excepții.	D
10.4.38.	SMAE ar trebui să accepte captura ca act a procesului de flux.	D
10.4.39.	Atunci când dosarele și actele au fost prelucrate folosind unul sau multe fluxuri de lucru, SMAE trebuie să permită utilizatorilor să stabilească identificatorii și versiunile fluxurilor utilizate.	D
10.4.40.	SMAE trebuie să se asigure că toate controalele de acces sunt păstrate în	P

Ref	Cerințe	Testabil
	orice moment. *Cu alte cuvinte, trebuie să fie imposibil de configurat vreun flux ce ar permite orice fel de acces vreunui utilizator care nu ar avea altfel drept de acces.*	
10.4.41.	SMAE ar trebui să fie compatibil cu modelul de referință al Workflow Management Coalition (WfMC).	D
10.4.42.	SMAE ar trebui să accepte exportul unui proces de flux standard sau a oricărei părți componente, conform cu orice schemă XML standardizată.	N
10.4.43.	Evidența de auditare a fluxului ar trebui să fie integrată cu evidența de auditare a SMAE.	D
10.4.44.	Evidența de auditare a fluxului trebuie să nu poată fi modificată.	D

10.5 Activități de caz

Această secțiune descrie cerințele pentru gestionarea „dosarelor de caz" într-un SMAE conform MoReq2. Vezi glosarul pentru o definiție și explicație asupra dosarelor de caz.

Termenul de „dosar de caz" este definit în glosarul MoReq2 ca un dosar care se referă la una sau mai multe tranzacții, desfășurate integral sau parțial într-o manieră structurată. În acest context, „structurat" semnifică faptul că tranzacțiile urmează reguli care sunt (sau pot fi) documentate, că ele urmează un proces riguros (care nu permite utilizatorilor să inoveze integral noi părți ale procesului) și ca ele sunt acțiuni repetate de-a lungul mai multor situații de tranzacții similare. Conținutul actelor din dosarele de caz pot fi structurate (de pildă, formulare completate online) sau nestructurate (de pildă, mesaje e-mail sau formulare pe hârtie scanate), în orice combinație; caracteristica esențială distinctivă a dosarelor de caz este că ele rezultă din procese structurate, cel puțin în parte.

Caracteristicile comune ale dosarelor de caz sunt:

- sunt în număr mare;
- sunt structurate sau parțial structurate;
- sunt folosite și administrate în cadrul unui proces cunoscut și prestabilit;
- trebuie să fie păstrate pentru perioade de timp prestabilite, ca rezultat al prevederilor legale sau regulamentare
- au un conținut/structură similare;
- au date de deschidere și închidere cunoscute;
- pot fi deschise sau închise de lucrătorii de caz (practicanți, personal angajat, sau sisteme de prelucrare a datelor) fără a fi nevoie de aprobarea conducerii;

Deoarece dosarele de caz sunt adesea structurate, ele conțin în general câteva sub-dosare, de obicei organizate prin intermediul unor șabloane. Ele pot de asemenea să conțină volume. Vezi secțiunea 3.3 pentru detalii asupra funcționalităților relevante, toate aplicându-se la dosarele de caz așa cum se aplică și altor tipuri de dosare.

Managementul de caz implică adesea și alte sisteme de aplicații pentru activități (de pildă, un sistem de prelucrare a licențelor de aplicații sau un sistem de urmărire a cercetării). De asemenea, adesea este dependent de fluxurile de lucru (așa cum au fost descrise în secțiunea 10.4).

Ref	Cerințe	Testabil
10.5.1	Un rol de administrator trebuie să poată configura SMAE astfel încât acesta să permită cel puțin un rol de „lucrător de caz” (vezi glosarul), cu particularitatea că rolul de lucrător de caz poate avea diferite permisiuni de acces pentru clasele cu sau fără lucrări de caz. *În multe cazuri, lucrătorii de caz vor fi capabili să creeze, deschidă și închidă dosare de caz ca parte a activității lor cotidiene, dar ei nu vor avea acea aprobarea de a crea deschide sau închide dosare generale. Pentru dosarele generale, autorizarea poate fi acordată doar rolurilor de administrator.*	D
10.5.2	SMAE ar trebui să accepte un mecanism opțional de stabilire a titlului dosarului, care să fie configurat de către un rol de administrator, care să includă nume (de pildă, nume de persoane) și/sau date (de pildă, datele de naștere) sau identificatori unici ca nume de dosare, derivate din și automat validate cu liste externe.	D
10.5.3	Aatunci când mecanismul de denumire este definit, metadatele utilizate pentru construcția automată a titlurilor de dosare (ca la 10.5.2) trebuie să fie metadate obligatorii sau elemente corespunzătoare implicite ar trebui să fie furnizate. Dacă valorile de metadate inițiale (de pildă, nume, date etc.) care au fost folosite pentru a crea titlul dosarului au fost modificate, SMAE nu ar trebui să actualizeze automat titlul dosarului.	D
10.5.4	Regulile pentru construcția automată a titlurilor de dosare (prevăzute la 10.5.2) ar trebui să fie configurabile pentru a fi diferite pentru diferite clase. *Ultimele trei cerințe pot fi corespunzătoare dosarelor de caz. Orice listă folosită pentru validare poate fi administrată din SMAE sau poate fi externă acestuia.* *Acolo unde un titlu de dosar a fost atribuit în mod automat folosind un mecanism care încorporează metadate, cum ar fi numele persoanei, data nașterii etc., este posibil ca această metadată originală pe care se bazează titlul să fie actualizată. De pildă, numele unei persoane se poate schimba, data nașterii se poate să fi fost introdusă greșit etc. În aceste situații, titlul dosarului bazat pe această metadată nu ar trebui să fie automat modificat*	D

Ref	Cerințe	Testabil

pentru a reflecta modificările, deoarece titlul dosarului poate să fi fost deja utilizat (de pildă în corespondență, înregistrare în alt sistem etc.). Dincolo de această cerință ca titlul dosarului să nu fie modificat, MoReq2 nu obligă la alte rezultate.

Câteva alte rezultate sunt posibile, aici incluzând:

- *schimbarea de metadate este ignorată și titlul dosarului rămâne același;*
- *un rol de administrator este alertat că metadata a fost actualizată și că rolul poate (opțional) să actualizeze titlul dosarului;*
- *utilizatorul care face schimbarea este avertizat că metadata a fost folosită în titlul dosarului și i se cere să confirme schimbarea metadatei;*
- *utilizatorul care face modificarea este împiedicat să actualizeze metadata și sfătuit să înainteze schimbările dorite către rolul de administrator, care poate să editeze metadata.*

10.5.5 SMAE trebuie să permită crearea de dosare de caz de către orice utilizator autorizat să fie lucrător de caz. D

10.5.6 SMAE trebuie să permită utilizatorilor să acceseze și să deschidă un dosar de caz prin introducerea identificatorului corespunzător de dosar de caz. D

În majoritatea dosarelor de caz, identificatorul de dosar, de pildă titlul sau numărul de referință, va fi furnizat de către un sistem extern. O interfață ar trebui să permită utilizatorului să valideze cu acesta un identificator introdus manual. Acesta este diferit și suplimentar față de identificatorul de sistem și codul de clasificare.

10.5.7 SMAE trebuie să furnizeze o Interfață de Programare a Aplicației (sau opțiuni similare), care să permită integrarea cu alte aplicații tip *business*. Aceasta trebuie să includă cel puțin următoarele funcționalități: P

- alte aplicații tip *business* să creeze, deschidă și închidă dosare de caz din SMAE ;
- alte aplicații tip *business* să furnizeze titlul dosarului de caz din SMAE ;
- codul de clasificare al unui dosar de caz nou creat să fie transferat către altă aplicație tip *business*;
- altă aplicație tip *business* să transfere actele pentru a fi declarate într-un dosar de caz din SMAE ;
- altă aplicație tip *business* să atribuie o programare de păstrare şi

Ref	Cerințe	Testabil
	dispoziţie unui dosar închis deja existent; ▪ gestionarea erorilor în cazul în care unul din sisteme inițiază o acțiune pe care celălalt o consideră nevalidă. *Este ca și cum aplicația tip* business *ar trebui să se comporte ca un utilizator obișnuit — SMAE nu ar trebui să facă vreo diferență între cei doi.* *MoReq2 nu specifică natura prelucrării erorilor. Cu toate acestea, rezultate specifice vor fi identificate în următoarele două cerințe.*	
10.5.8	SMAE trebuie, la primirea unei cereri din partea unei aplicații tip *business* externă, care pare a fi nevalidă: ▪ să nu încheie nici o acțiune nevalidă; ▪ să nu genereze blocaje nici în SMAE, nici în aplicația externă.	D
10.5.9	SMAE ar trebui, la primirea unei cereri din partea unei aplicații tip *business* externă, care pare a fi nevalidă, să alerteze un utilizator autorizat astfel încât acțiunile de corectare să poată fi întreprinse.	D
10.5.10	Atunci când SMAE interferează cu o altă aplicație tip *business,* trebuie să fie posibil ca rolul de administrator să limiteze acțiunile celeilalte aplicații la una sau mai multe clase specificate, în cadrul schemei de clasificare a SMAE. *Altfel spus, trebuie să fie imposibil pentru o altă aplicație să întreprindă orice fel de acțiune care afectează clasele, dosarele sau actele, în afara clasei(lor) care conțin dosarele de caz.*	D
10.5.11	Atunci când SMAE interferează cu altă aplicație tip *business*, ar trebui să fie posibil ca un utilizator să comute ușor între dosarele înrudite din ambele aplicații *Altfel spus, un utilizator care a folosit caracteristicile celeilalte aplicații tip business pentru a localiza sau identifica un caz sau un dosar de caz (de pildă, folosind caracteristica aplicației de căutare a unui cod poștal pentru a identifica un anume caz) trebuie să poată deschide cu ușurință dosarul de caz în SMAE, adică fără a fi nevoit să re-tasteze identificatorul dosarului de caz. În mod asemănător, un utilizator care a deschis un dosar de caz în SMAE (prin parcurgerea schemei de clasificare, prin căutare sau prin orice alt mijloc) trebuie să poată comuta în același mod către informația de caz corespondentă din cealaltă aplicație tip* business*.*	N
10.5.12	Acolo unde SMAE permite unei alte aplicații tip *business* să creeze noi dosare de caz, el trebuie să poată primi metadatele de dosar relevante care sunt specifice dosarelor de caz.	D

Ref	Cerințe	Testabil
10.5.13	SMAE trebuie să permită ca dosarele de caz să fie configurate cu elemente de metadate care sunt specifice dosarelor de caz. *De exemplu, un dosar de caz poate avea nevoie de unul sau mai multe elemente de metadate care să indice „starea" sau „progresul".*	D
10.5.14	SMAE trebuie să permită utilizatorilor să regăsească, să declare acte și să desfășoare toate celelalte acțiuni valide asupra dosarelor de caz, prin folosirea unui identificator de dosar de caz în locul codului de clasificare. *Majoritatea dosarelor de caz sunt identificate printr-un identificator de caz unic cum ar fi un numărul contului sau numărul plângerii. Utilizatorii trebuie să poată lucra cu aceste dosare prin specificarea identificatorului și fără a fi nevoie să folosească codul de clasificare al SMAE (deși această posibilitate rămâne deschisă).*	P
10.5.15	Atunci când SMAE primește acte cu un conținut structurat din altă aplicație tip *business*, trebuie să poată extrage automat metadate din acte.	D
10.5.16	Atunci când SMAE primește acte cu un conținut structurat din altă aplicație tip *business*, trebuie să poată folosi metadatele extrase pentru a declara actele în dosarul corespunzător. *De pildă, dacă un SMAE primește formulare electronice de solicitări dintr-o aplicație de prelucrare a cererilor de beneficii, ar trebui să poată extrage identificatorul solicitantului și genul de formular, apoi să le folosească pentru clasificarea formularelor în dosarul (folosind identificatorul solicitantului) și sub-dosarul (folosind genul de formular) corespunzător.*	D
10.5.17	SMAE trebuie să se asigure că toate acțiunile desfășurate asupra oricărei clase, dosar sau act, fie de utilizatorul autorizat, fie de o altă aplicație tip *business*, sunt înregistrate în evidența de auditare.	D
10.5.18	SMAE trebuie să fie capabil să producă rapoarte despre toate acțiunile desfășurate asupra oricărui câmp/câmpuri, fie de un utilizator autorizat, fie de o altă aplicație tip *business.*	D
10.5.19	SMAE trebuie să poată produce rapoarte pentru rolurile de administrator, prezentând cel puțin: ▪ numărul de acte declarate în mod automat în dosarele de caz din aplicații de tip business, pe o perioadă de timp dată; ▪ numărul de acte declarate în mod manual în dosarele de caz, pe o perioadă de timp dată; ▪ numărul de dosare de caz deschise și închise automat de alte	D

Ref	Cerințe	Testabil

sisteme tip *business*, pe o perioadă de timp dată;

- numărul de dosare de caz deschise și închise manual pe perioadă de timp.

10.6 Integrarea cu Sisteme de Management al Conținutului

Această secțiune tratează cerințele pentru integrarea Sistemelor de Management al Conținutului (Content Management System, CMS) cu SMAE. Sistemele moderne de CMS includ cele mai multe sau toate funcționalitățile unui SMDE (vezi secțiunea 10.3). Această secțiune tratează doar cerințele funcționale ale unui CMS pentru un SMAE — nu descrie cerințele funcționale pentru CMS sau SMDE și nici nu include suficiente funcționalități pentru a face funcționalitățile SMAE să îndeplinească sarcini asociate în mod normal cu CMS.

CMS include și extinde funcționalitățile SMDE pentru toate formele de informație (conținut), nu doar pentru acte. CMS se ocupă, în mod obișnuit, de aspecte ale administrării informației diferite de un cele ale SMAE. Caracteristicile comune sunt:

- publicarea informației, adesea pe website-uri sau prin portaluri, și uneori pe diferite canale, folosind diferite forme de redare.
- administrarea informației care provine din diferite surse;
- reformatarea informației și/sau migrarea ei către diferite forme de redare;
- relaționarea reciprocă diferitelor versiuni, redări sau traduceri de documente;
- administrarea componentelor de documente.

La momentul redactării, cea mai frecventă utilizare a termenului de CMS și cea mai frecventă nevoie de integrare cu SMAE par a fi aplicate la publicarea web. Cu toate acestea, prezenta secțiune este destinată atât publicării web, cât și altor feluri de CMS.

Funcționalitățile de management al conținutului pot fi furnizate de un CMS separat de un SMAE, sau printr-un pachet integrat care furnizează atât funcționalități CRM, cât și management de acte electronice. Pentru simplificarea explicației, această secțiune descrie cerințele MoReq2 ca și cum CMS și SMAE ar fi separate; această separare nu este o cerință.

Relația între SMAE și CMS este prezentată, într-o formă extrem de simplificată, în figura 10.1.

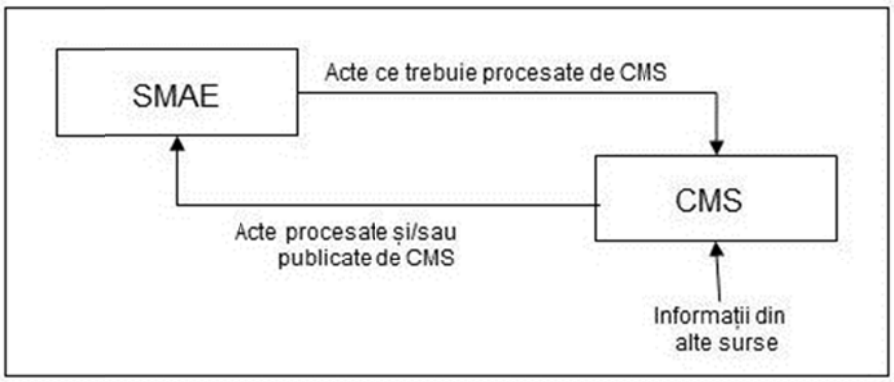


Figura 10.1

Această figură indică:

- copiile actelor pot fi transferate din SMAE în CMS pentru prelucrare (prelucrarea implică de obicei editare, migrarea către diferite redări și publicarea).
- actele pot fi transferate din CMS în SMAE pentru capturare. Aceasta se poate produce în timp ce informația este prelucrată de CMS, sau după ce a fost prelucrată și publicată. Actele pot include (printre altele) pagini web, website-uri și noi redări ale actelor existente;

CMS poate de asemenea primi informații din alte surse, astfel încât actele pe care le transferă înapoi spre SMAE pot consta dintr-o combinație de informații care își au originea în SMAE și informații din alte părți.

De reținut că expresia: „poate fi transferat…" acoperă câteva posibilități:

- copii ale actelor sunt transmise între aplicații;
- actele sunt stocate într-un depozit care este comun pentru CMS și SMAE și doar mesajele de identificare a documentelor și actelor sunt transmise între aplicații;
- actele sunt stocate într-un depozit care este comun pentru CMS și SMAE și ambele acționează asupra lor fără a mai fi nevoie să transmită vreo informație.

În această secțiune, „transferul de copii" se poate referi la oricare din aceste scenarii (sau la unele asemănătoare). Tehnologia CMS se evoluează rapid, astfel încât organizațiile care au nevoie de integrare cu CMS trebuie să specifice cerințele lor individuale; folosirea doar a prezentei secțiuni ce mai probabil nu va fi suficientă. Această secțiune ar trebui văzută ca un punct de plecare, pentru a genera analize ulterioare.

Ref	Cerințe	Testabil
10.6.1	SMAE trebuie să poată primi acte din partea CMS, inclusiv metadatele specificate, și trebuie: ▪ fie să captureze automat actele în câmpurile corespunzătoare bazate pe metadatele lor; ▪ fie să permită utilizatorului să specifice câmpurile corespunzătoare.	Y
10.6.2	SMAE trebuie să poată captura ca acte componente specifice CMS și tipuri de fișiere, incluzând: ▪ fișiere jurnal ale administrației conținutului; ▪ foi de stil	Y
10.6.3	SMAE trebuie să găzduiască metadatele cerute de CMS, pe lângă metadatele necesare pentru managementul actelor, specificate de MoReq2.	Y

Ref	Cerințe	Testabil
	De pildă, un CMS poate folosi elemente de metadate pentru a stoca informații necesare pentru managementul conținutului, cum ar fi: ▪ *adresa IP;* ▪ *starea;* ▪ *limba;* ▪ *data publicării;* ▪ *data efectivă;* ▪ *motivele modificării.* *SMAE trebuie să poată stoca aceste elemente, chiar dacă ele nu sunt cerute pentru managementul actelor. Nu este necesar ca SMAE să poată stoca toate metadatele produse sau folosite de CMS; este nevoie ca doar elementele specificate în momentul configurării să fie stocate. Elementele care urmează să fie stocate trebuie să fie stabilite în baza nevoilor activității.* *De remarcat că aceasta este o cerință extrem de generală. Ea permite ca o mare varietate de funcții să fie desfășurate de CMS și apoi stocate ca metadate în SMAE.*	
10.6.4	Atunci când un act este transferat din CMS către SMAE în vederea capturării, dacă acel act este asociat cu un act existent stocat în SMAE (de pildă, este o redare sau traducere diferită a unui act existent) SMAE nu trebuie să șteargă sau să modifice actul existent, ci trebuie să stocheze noul act.	P
10.6.5	Atunci când un act asociat cu un act existent (la fel ca la 10.6.4) este transferat din CMS în SMAE pentru capturare, SMAE trebuie să lege în mod automat actul existent și cel nou (ca în 3.4.23). *Această cerință va fi posibilă doar dacă CMS transferă, odată cu actul, identificatorul actului existent, ca valoare de metadată. Dacă CMS nu transferă înapoi această valoare, atunci SMAE nu poate eșua în testul de conformitate MoReq2.*	Y
10.6.6	Atunci când un act asociat cu un act existent (ca în 10.6.4) este transferat din CMS în SMAE și apoi capturat ca act, SMAE ar trebui să se asigure că metadatele noului act sunt, pe cât posibil, identice cu cele ale actului original prin legarea lui la aceleași metadate, având ca diferențe relevante în metadate doar pe cele care sunt cerute pentru a înregistra schimbările și acțiunile CMS.	N
10.6.7	Atunci când documentele sunt transferate din CMS în SMAE sub formă de pagini web, SMAE ar trebui să poată să captureze o pagină web sau un set	Y

Ref	Cerințe	Testabil
	de pagini web, declarându-le un singur act. *Capacitata de a captura un set de pagini ca un singur act poate fi utilă în câteva situații, cum ar fi stocarea periodică de copii instantanee (*snapshot*) ale unui web site.* *Capturarea paginilor web este probabil să solicite și schimbări în referințe (hiper-legături din cadrul paginilor, hiper-legături spre alte pagini web, și referințe la elemente grafice și alte componente etc.), astfel încât să permită paginilor să fie corect afișate și să păstreze cât de mult posibil din funcționalitatea lor originală. Aceasta este de inevitabilă dacă paginile web care includ elemente grafice, foi de stil, hiper-legături etc. trebuie stocate în formatul original fără pierderea tuturor funcționalităților și fidelității. Aspectul cheie este că, conținutul furnizor de informație al paginii web nu trebuie să fie modificat. Vezi cerințele 6.3.5 și 6.3.5.*	
10.6.8	Atunci când actele sunt primit de SMAE dintr-un CMS, aceasta trebuie să se înregistreze automat în evidența de auditare a SMAE și în metadatele actului.	Y
10.6.9	Atunci când un utilizator selectează actele care trebuie copiate de SMAE în CMS, SMAE trebuie să permită utilizatorului să folosească orice valoare de metadată disponibilă din CMS ca bază pentru selectarea actelor care trebuie transferate. *Pentru a continua exemplul din 10.6.3, un utilizator poate selecta actele într-o clasă specificată cu specificarea valorilor de „dată efectivă” și „stare”.*	Y
10.6.10	SMAE trebuie să permită utilizatorilor să inițieze transferul copiilor actelor specificate, împreună cu metadatele specificate, din SMAE în CMS. *Metadatele care trebuie să fie transferate pot fi specificate în momentul configurării sistemului.*	Y
10.6.11	Atunci când actele sunt transferate din SMAE către CMS, aceasta trebuie să fie înregistrată automat în evidența de auditare a ERS și în metadatele actelor.	Y

10.7 Semnătura electronică

Semnăturile electronica (uneori numite şi semnături digitale) constau dintr-o informaţie care este ataşată de, sau este logic asociată cu alte informaţii, cum ar fi un act electronic, şi care serveşte ca metodă de autentificare. Semnătura electronică ia în mod obişnuit forma unei secvenţe de caractere. Este folosită cu algoritmi de siguranţă, proceduri şi „chei” (un sir lung de caractere similar unei parole) pentru a confirma integritatea unui act şi/sau să autentifice identitatea expeditorului sau sursa unui act. Semnătura electronică nu ar trebui confundată cu o imagine

bitmap sau scanată a unei semnături pe hârtie — aceasta nu este considerată sigură, şi astfel este puţin probabil să furnizeze o probă a autenticităţii unui act.

O semnătură electronică, în sensul MoReq2, este o formă de „semnătură electronică extinsă”, aşa cum este definită în Directiva europeană asupra unui Cadru Comunitar pentru semnăturile electronice 1999/93/EC. O semnătură electronică extinsă este una care este conformă cu definiţia din Directivă, şi anume că semnătura este:

- asociată în mod unic cu semnatarul;
- capabilă să identifice semnatarul;
- este creată folosind mijloace pe care semnatarul le poate păstra doar sub controlul său;
- este asociată cu date (de pildă, un act) de care este legată astfel încât orice modificare ulterioară a datelor (de pildă, un act) este detectabilă.

Un alt standard, neînrudit, pentru cadrul semnăturii electronice este X.509 (vezi anexa 7).

Exemple de algoritmi de semnătură electronică larg recunoscuţi sunt Algoritmul de Semnătură Electronică (DSA) aşa cum este definit în FIPS 186-2 (vezi anexa 7) şi RSA/SHA-1.

E-mail-ul a devenit mijlocul de bază de comunicare pentru multe organizaţi şi acesta a determinat o largă mişcare de documente şi acte într-un mediu relativ necontrolat. Folosirea semnăturii electronice pentru autentificare şi confirmarea integrităţii a devenit, prin urmare, larg adoptată, mai ales acolo unde acte ale tranzacţiilor economice sunt implicate.

Semnăturile electronice sunt de asemenea larg folosite pentru a proba caracterul non-repudiabil — repudierea se referă la orice acţiune de neasumare a responsabilităţii pentru un mesaj. Non-repudierea furnizează dovada integrităţii şi originii datelor, care poate fi verificată de un terţ în orice moment. Astfel o persoană sau o entitate este împiedicată să nege că a desfăşurat o anumită acţiune legată de acele date, cum ar fi aprobarea, transmiterea, primirea, luarea la cunoştinţă (recunoaşterea conţinutului unui mesa primit) sau livrarea (primire şi luare la cunoştinţă).

Cerinţele din această secţiune se aplică doar acolo unde există o cerinţă de a administra actele ce poartă semnături electronice. La momentul redactării, semnătura electronică este încă subiect a dezbaterilor şi incertitudinilor, pe măsură ce noi infrastructuri şi algoritmi sunt testaţi şi implementaţi. Această stare de lucruri tinde să se continue. Utilizatorii MoReq2 ar trebui prin urmare să îşi verifice cerinţele şi implicaţiile pentru păstrare pe termen lung cu autorităţile competente.

Nu există nici o cerinţă în această secţiune care să se refere la o anumită legislaţie naţională referitoare la semnătura electronică. Spre exemplificare, anumite legi impun ca semnătura să fie păstrată complet pentru a avea valoare, în timp ce altele impun doar păstrarea metadatelor referitoare la o semnătură. Acolo unde asemenea cerinţe sunt relevante, ele pot fi tratate în Capitolul Zero, specific naţional.

Ref	Cerinţă	Testabil
10.7.1	La momentul capturării actului, SMAE trebuie să poată captura, verifica dacă este cerut şi stoca semnăturile electronice, certificatele electronice asociate şi detaliile despre furnizori de servicii de certificare.	D

Ref	Cerinţă	Testabil
	Această cerinţă este esenţială de vreme ce nu va fi întotdeauna posibil să se re-creeze aceste informaţii la un moment viitor.	
10.7.2	SMAE trebuie să permită rolurile de administrator să configureze sistemul, fie în momentul configurării sistemului, fie la un moment ulterior, astfel încât acesta să stocheze la momentul capturii metadatele de verificare pentru actele semnate electronic, inclusiv cheile publice, împreună cu actele, în una din următoarele forme: ▪ faptul unei verificări de succes; ▪ informaţia specificată referitoare la procesul de verificare; ▪ toate datele de verificare. *Această cerinţă este esenţială de vreme ce nu va fi întotdeauna posibil să se re-creeze aceste informaţii la un moment viitor.*	D
10.7.3	SMAE ar trebui să aibă o interfaţă bazată pe standarde care să permită introducerea noilor tehnologii de semnătură electronică, pe măsură ce ele sunt introduse. *Un exemplu de bază standardizată potrivită este XML Key Management Spec (XKMS, vezi anexa 7).* *Această cerinţă este în special relevantă, date fiind schimbările ce intervin în acest sector.*	N
10.7.4	SMAE ar trebui să fie capabil să verifice validitatea unei semnături electronice, inclusiv verificarea certificatului unui act la momentul capturării, într-o listă de revocare a certificatelor electronice şi ar trebui să stocheze rezultatul verificării în metadatele actului. *Această cerinţă este relevantă deoarece nu va fi întotdeauna posibil să se desfăşoare aceste verificări la un moment viitor.*	D
10.7.5	Atunci când capturează mesajul e-mail, SMAE trebuie să poată captura în mod automat, şi să prezerve ca metadate, detalii despre procesul verificării pentru semnătură electronică, incluzând: ▪ faptul că validitatea semnăturii a fost verificată; ▪ identitatea persoanei care a iniţiat verificarea (acolo unde este relevant); ▪ emitentul certificatului; ▪ numărul de serie al certificatului electronic, care a verificat semnătura; ▪ furnizorul serviciului de verificare cu care a fost verificată	D

Ref	Cerinţă	Testabil
	semnătura; ▪ data şi ora la care s-a produs verificarea. *Această cerinţă este esenţială, de vreme ce nu va fi întotdeauna posibil să fie re-create aceste informaţii la un moment viitor. Din cauza modificărilor de software, din cauza expirării certificatelor şi datorită autorităţilor externe care îşi pot înceta activitatea, nu se poate garanta verificarea semnăturilor pe termen lung; de aici această cerinţă de a înregistra faptul că o semnătură a fost verificată cu succes.*	
10.7.6	SMAE ar trebui să includă caracteristici care demonstrează că integritatea actelor purtătoare de semnătură electronică a fost menţinută. *Un exemplu ar putea fi verificarea unei semnături electronice. Această demonstrare a integrităţii ar trebui să se aplice chiar dacă un rol de administrator a efectuat modificări autorizate în metadatele actului.* *Felul în care această cerinţă poate fi realizată nu este precizat.*	N
10.7.7	SMAE ar trebui să poată stoca împreună cu actul electronic: ▪ semnătura electronică asociată cu acel act; ▪ certificatul electronic care verifică semnătura.	D
10.7.8	Ar trebui să fie posibil ca un administrator de SMAE să definească dacă SMAE va stoca biletul de validare returnat de sistemul care a verificat semnătura electronică. *Biletul de validare este uneori numit* token*.*	D
10.7.9	SMAE ar trebui să permită unui rol de administrator să aplice o semnătură electronică unui dosar sau unui act sau unui mesaj de transfer în timpul unui proces de export sau transfer, astfel încât integritatea şi originea dosarului, actului sau mesajului de transfer să poată fi verificată ulterior. *Un mesaj de transfer este un mesaj transmis între sisteme ca parte a unui protocol folosit pentru a administra transferurile dintre sisteme.*	D
10.7.10	O semnătură electronică aplicată în timpul exportului sau transferului (vezi 10.7.10) ar trebui să fie capabil de validare externă, astfel încât integritatea şi originea dosarului, actului sau mesajului de transfer să poată fi verificată ulterior. *Pentru a realiza acest lucru, SMAE trebuie să fie capabil să exporte un certificat electronic cu cheia publică a organizaţiei împreună acu actul.*	D

10.8 Criptarea

Criptarea este procesul de aplicare a unei transformări complexe asupra unui obiect electronic, astfel încât acesta să nu fie prezentat de o aplicaţie într-o formă lizibilă sau inteligibilă, exceptând cazul în care transformarea corespondentă de decriptare a fost aplicată. Aceasta poate fi folosită pentru a securiza obiectele electronice, prin folosirea transformărilor care cer utilizarea de coduri de chei electronice securizate.

Cerinţele din această secţiune se aplică doar dacă există cerinţe de administrare a actelor care sunt criptate.

Ref	Cerinţă	Testabil
10.8.1	Acolo unde un act electronic a fost trimis sau primit într-o formă criptată printr-o aplicaţie care interferează cu SMAE, acesta din urmă trebuie să fie capabil să permită accesul la acel act doar utilizatorilor listaţi ca deţinând cheia de decriptare relevantă, în plus faţă de orice altă formă de restricţie atribuită acelui act.	Y
10.8.2	SMAE trebuie să poată captura şi stoca, la momentul capturii actului, informaţii referitoare la criptare şi la detalii ale agenţiilor de verificare asociate.	Y
10.8.3	Acolo unde un act electronic a fost transmis în formă criptată de către o aplicaţie care interferează cu SMAE, SMAE ar trebui să poată păstra ca metadate împreună cu actul: ▪ faptul transmiterii criptate; ▪ numărul de serie al certificatului electronic (acolo unde este cazul); ▪ tipul de algoritm; ▪ nivelul de criptare folosit; ▪ data şi ora procesului de criptare şi/sau decriptare, acolo unde este cazul.	Y
10.8.4	SMAE ar trebui să poată permite captura actelor criptate dintr-o aplicaţie care are capacităţi de criptare.	Y
10.8.5	SMAE ar trebui să permită înlăturarea criptării atunci când un act este importat sau capturat. Această caracteristică ar trebui să fie configurată de către un rol de administrator în momentul configurării sistemului sau mai târziu. *Această caracteristică poate fi dorită în anumite arhive istorice de mari dimensiunii, care au cerinţe pentru acces pe termen lung (din cauza criptării etc. este probabilă reducerea capacităţii de a citi actele pe termen lung). În acest caz, organizaţia s-ar putea baza pe evidenţa de auditare sau pe*	Y

Ref	Cerinţă	Testabil
	informaţii similare pentru a demonstra că criptarea etc. a fost prezentă dar a fost înlăturată. În alte medii, această caracteristică poate să nu fie dorită, din punct de vedere legal. Vezi secţiunile 5.3 şi 3.1 pentru mai multe detalii asupra transferului şi importării.	
10.8.6	SMAE ar trebui să aibă o structură care să permită să fie introduse noi tehnologii.	N

10.9. Administrarea drepturilor digitale

Acest modul opţional nu cuprinde nici o cerinţă care să poată fi testată în forma sa actuală. Aşa cum este explicat mai jos, testarea va avea relevanţă doar dacă cerinţele vor fi adaptate tehnologiilor specificate.

Administrarea drepturilor digitale (Digital Rights Management, DRM) şi Administrarea drepturilor digitale de companie (Enterprise Digital Rights Management, uneori prescurtată E-DRM) constituie un set de tehnologii încă nestandardizate folosite pentru a proteja proprietatea intelectuală şi/sau pentru a restricţiona distribuirea informaţiei. DRM este în general asociat cu protecţia drepturilor intelectuale (în special în industria muzicii, a publicaţiilor electronice şi a filmului), în timp ce E-DRM este în general asociat cu implementarea restricţiilor asupra distribuţiei informaţiilor legate de activităţi, pentru raţiuni de securitate sau secrete comerciale. Cu toate acestea, limitele nu sunt precise şi ambele pot fi întâlnite în contextul unui SMAE. În consecinţă, în contextul prezentei secţiuni, aceste tehnologii vor fi denumite DRM/E-DRM.

Exemple de DRM/E-DRM includ:

- Filigranare electronică (numită uneori şi filigranare digitală) care înglobează informaţii vizibilă despre proprietatea drepturilor intelectuale în acte sau documente. Informaţia este introdusă de o o manieră care să facă dificilă eliminarea lui.
- Steganografie, care introduce de o manieră similară informaţie despre drepturile intelectuale, dar într-un sistem invizibil, sau, în cazul unui fişier audio, un sistem care nu poate fi auzit. Este necesar un program special pentru a citi informaţiile despre drepturile intelectuale.
- Scheme de protecţie împotriva copierii, care folosesc o varietate de abordări pentru a împiedica copierea.
- Caracteristici incluse în documente sau acte care permit acestora sa fie vizualizate, dar nu imprimate.
- Caracteristici de ,,expirare” incluse în acte sau documente, care le împiedică să fie prezentate în orice fel după ce data specificată a fost depăşită.

Tehnologiile DRM/E-DRM sunt la un nivel relativ incipient de dezvoltare. Ele sunt previzibil supuse schimbărilor în perioada de existenţă estimată a MoReq2.

Aceste tehnologii, precum şi altele similare, pot fi aplicate la acte în mai multe formate, inclusiv înregistrări audio şi video digitalizate.

Aceste tehnologii generează o provocare specială în managementul actelor, de vreme ce ele pot face dificilă sau chiar imposibilă prezentare ulterioară a actelor. De pildă:

- Unele forme de filigran se bazează, pentru a putea fi efective, pe prezenţa unor aplicaţii complementare (*plug-în)* în aplicaţia de vizualizare. Un act cu un astfel de filigran poate fi vizualizat fără complementar, dar nu va fi posibilă obţinerea tuturor informaţiilor din filigran dacă nu este disponibil programul complementar. Cu trecerea timpului, creşte probabilitatea ca acest program să nu mai fie disponibil.
- Un mesaj e-mail conţine o setare de expirare şi el nu va mai putea fi citit după o anumită dată. Această problemă este în mod particular perfidă, deoarece nu va fi identificabilă în momentul capturării actului.

Ca cerinţă minimală, rolurile de administrator şi utilizator responsabile de captura şi managementul actelor electronice trebuie să fie avizaţi de orice caracteristică DRM/E-DRM care afectează actele din SMAE. Alte potenţiale dificultăţi în managementul actelor, provocate de aceste tehnologii, pot fi reduse dacă acele caracteristici DRM/E-DRM sunt eliminate din acte la momentul capturării sau imediat după. Cu toate acestea, ambele abordări sunt aspecte procedurale şi, ca urmare, dincolo de cadrul MoReq2.

Tehnologiile aplicabile variază extreme de larg, şi efectul lor asupra actelor variază cu aceeaşi amploare. Din acest motiv, nu este posibil să fie formulate cerinţe generice, aplicabile tuturor tehnologiilor. Ca urmare, această secţiune specifică o serie de cerinţe de nivel general, care vor trebui dezvoltate de utilizatorii MoReq2 dacă acestea trebuie utilizate pentru specificaţii şi achiziţie. Deci, de pildă, dacă se întrevede posibilitatea de existenţă a acelei caracteristici de expirare, cerinţele trebuie adaptate pentru a genera cerinţe specifice care să gestioneze caracteristica de expirate.

Ref	Cerinţă	Testabil
10.9.1	SMAE trebuie să fie capabil să captureze şi să stocheze acte ce prezintă caracteristici DRM/E-DRM.	N
10.9.2	SMAE ar trebui să poată identifica prezenţa caracteristicilor DRM/E-DRM într-un act la momentul capturării. Acolo unde caracteristici DRM/E-DRM au fost identificate, SMAE ar trebui să notifice utilizatorul şi să furnizeze următoarele opţiuni: ▪ păstrează caracteristicile DRM/E-DRM; ▪ înlătură caracteristicile DRM/E-DRM; ▪ opreşte procesul de captură.	N
10.9.3	SMAE ar trebui să poată elimina caracteristicile DRM/E-DRM din acte în timpul capturii.	N

Ref	Cerinţă	Testabil
	Această cerinţă poate fi obligatorie în anumite medii, dar nu poate fi general obligatorie, deoarece ar cere o posibilitate arbitrară de a ocoli caracteristicile de securitate. Dacă acele caracteristici DRM/E-DRM sunt eliminate, această acţiune trebuie înregistrată în evidenţa de auditare.	
10.9.4	SMAE ar trebui să includă posibilitatea de a controla accesul la acte pe baza restricţiilor de proprietate intelectuală şi să genereze date de taxare pentru asemenea accesări. *Această scurtă declaraţie acoperă o sferă largă de funcţionalităţi, care sunt situate în afara domeniul MoReq2. Această cerinţă poate fi satisfăcută prin furnizarea posibilităţii de legătură cu a aplicaţie separată.*	N
10.9.5	SMAE ar trebui să fie capabil să prezinte corect acte cu caracteristici DRM/E-DRM, în măsura în care caracteristicile DRM/E-DRM permit acest lucru.	N
10.9.6	SMAE ar trebui să poată regăsi şi stoca la momentul declarării informaţii stocate în caracteristicile DRM/E-DRM, în măsură în care caracteristicile DRM/E-DRM permit. *De pildă, identitatea deţinătorului dreptului de proprietate intelectuală, aşa cum este codificat în filigran; sau data expirării.* *Această cerinţă poate fi obligatorie în anumite medii, dar nu poate fi general obligatorie, deoarece ar cere o posibilitate arbitrară de a ocoli caracteristicile de securitate.*	N
10.9.7	SMAE ar trebui să permită ca noile tehnologii DRM/E-DRM să fie introduse.	N
10.9.8	SMAE ar trebui să poată aplica actelor caracteristici DRM/E-DRM în timpul exportării. *Această cerinţă este de dorit mai ales în situaţia în care caracteristicile DRM/E-DRM au fost eliminate.*	N

10.10 Sisteme dispersate

Această secțiune cuprinde cerințe pentru organizațiile care au nevoie de un SMAE care să opereze în mai multe locuri.

Multe organizații își desfășoară activitatea în mai multe sedii. Acolo unde sediile sunt relativ apropiate spațial unul de celălalt, sau atunci când conexiunea de rețea între toate sediile este bună (cu o capacitate suficientă), este posibil ca o singură instanță a unui SMAE să fie cea mai potrivită pentru a deservi toate sediile. În aceste cazuri, toate structurile operează ca și cum ele s-ar afla în același loc și nu este nevoie ca cerințele din această secțiune să fie aplicate. Cu toate

acestea, dacă sediile sunt separate net, și/sau dacă conexiunea între ele nu este bună, atunci ar putea fi necesar să se implementeze un SMAE dispersat; în acest caz, se aplică cerințele din această secțiune.

Există câteva abordări arhitecturale diferite ale sistemelor dispersate. Acestea includ o instanță a unui SMAE care controlează mai multe depozite; mai multe instanțe ale unui SMAE fiecare cu propriul său depozit, comunicând între ele; și alte abordări. MoReq2 nu precizează o abordare arhitecturală; el specifică doar cerințele cheie pentru asemenea medii dispersate și folosește termenul de „ SMAE dispersat” pentru a denumi o astfel de arhitectură.

Ref	Cerință	Testabil
10.10.1	SMAE trebuie să fie capabil să fie configurat de un rol de administrator pentru a fi folosit din multiple sedii.	N
10.10.2	SMAE ar trebui să accepte o schemă de clasificare dispersată de-a lungul unei rețele de depozite de acte electronice.	D
10.10.3	SMAE trebuie să permită unui rol de administrator să asigure mentenanța claselor, dosarelor, sub-dosarelor, volumelor, actelor, a metadatelor asociate lor și a evidențelor de auditare în cadrul unui SMAE dispersat, astfel încât operațiunile de mentenanță să poată fi desfășurate o singură dată și să fie aplicate pe întregul SMAE dispersat. *Mentenanța presupune desfășurarea de tranzacții, așa cum este specificat în capitolul 3, secțiunea 9.1 și în alte părți.*	P
10.10.4	Acolo unde SMAE acceptă depozite multiple, ar trebui să permită ca un rol de administrator saă precizeze care depozit stochează exemplarul master al fiecărei clase (și clasele sale fiică, respectiv actele clasate în ele etc.) *De pildă, o organizație poate decide să implementeze un depozit pentru fiecare din sedii, actele fiecărui sediu fiind stocate în depozitul local (aceasta presupune că proiectul schemei de clasificare accepta configurația).*	D
10.10.5	Acolo unde SMAE acceptă depozite multiple, ar trebui să permită unui rol de administrator să precizeze care depozit(e) stochează automat o copie a fiecărei clase (și ale claselor fiică, a actelor clasate în ele etc.). *De exemplu, o organizație poate decide că;* ▪ *toate depozitele trebuie să fie copiate în depozitul de la sediul central;* ▪ *într-o anumită zonă geografică, toate depozitele trebuie să fie copiate reciproc.* *De observat că această cerință înseamnă implicit că depozitele trebuie să fie*	D

Ref	Cerință	Testabil
	sincronizate automat. Aceasta include depozitele de: ▪ *acte și documente;* ▪ *metadate.*	
10.10.6	Acolo unde SMAE acceptă mai multe depozite, ar trebui să permită unui rol de administrator să precizeze care depozit(e) pot fi accesat de utilizatori la fiecare sediu. *De exemplu, organizația poate decide că:* ▪ *toți utilizatorii pot avea acces doar la depozitul pentru sediul lor;* ▪ *toți utilizatorii pot avea acces doar la depozitul pentru sediul lor și pentru sediul central;* ▪ *toți utilizatorii din sediul central pot avea acces la orice depozit, în timp ce toți ceilalți utilizatori pot avea acces doar la depozitul pentru sediul lor;* ▪ *toți utilizatorii pot ava acces la toate depozitele din zona lor geografică (de pildă, în cadrul unui set specificat de depozite; aceasta nu înseamnă că SMAE trebuie să recunoască conceptul de „zonă geografică”),*	D
10.10.7	Acolo unde SMAE acceptă depozite multiple, ar trebui să permită unui rol de administrator să specifice că toate evidențele de auditare vor fi copiate într-un singur depozit.	D
10.10.8	SMAE trebuie să împiedice sau să rezolve orice conflict generat de schimbări produse la diferite sedii. *De pildă, un potențial conflict poate apare dacă două roluri de administrator din sedii diferite fac schimbări diferite în metadatele aceleiași clase, care este stocată într-un alt treilea sediu.*	P
10.10.9	SMAE trebuie să permită unui rol de administrator să monitorizeze atât întregul SMAE dispersat ca pe o singură entitate, cât și depozitele individuale, furnizând aceleași facilități ca cele descrise în secțiunea 9.2.	D
10.10.10	SMAE trebuie să poată produce rapoarte (după cum este specificat în secțiunea 9.2) care să acopere depozite multiple.	D
10.10.11	SMAE ar trebui să accepte memorarea celor mai frecvent și recent folosite dosare, sub-dosare, volume și acte, accesat din sedii folosind depozitele de la distanță. *Următoarele două cerințe se referă la performanța SMAE dispersate. Se va folosi convenția de a exprima cantități variabile în paranteze unghiulare (de*	D

Ref	Cerință	Testabil
	pildă <xx minute/ore>, așa cum este explicat în introducerea la capitolul 11.	
10.10.12	Acolo unde SMAE sincronizează depozitele, ele trebuie să fie sincronizate într-un interval de <xx minute/ore> de la orice schimbare (în funcție de disponibilitatea conexiunii de rețea).	N
10.10.13	*SMAE trebuie să fie capabil să transmită orice modificare administrativă în cadrul tuturor depozitelor într-un interval de <xx minute/ore>* *Cerințele 10.10.12 și 10.10.13 sunt cerințe exemplu. MoReq2 nu precizează timpul de răspuns deoarece el este dependent de sistem. Vezi secțiunea 11.2 pentru o descriere completă.* *Este esențial ca arhitectura sistemului să permită timpi de răspuns acceptabili pentru toate sediile. Utilizatorii MoReq2 ar trebui să ia în considerare specificarea timpilor de răspuns pentru multe din cerințele specificate în secțiunea 11.2, separat pentru tranzacțiile implicând informații păstrate în depozite la distanță.*	N
10.10.14	Acolo unde SMAE este capabil să creeze fluxuri de lucru în cadrul sistemelor dispersate, el trebuie să fie capabil să facă schimb de date între aceste sisteme pentru a controla procesul de flux.	D
10.10.15	Acolo unde SMAE acceptă depozite multiple, și acolo unde exemplarele master sunt stocate în depozitele specificate (vezi 10.10.4), el ar trebui să permită unui rol de administrator să modifice care depozit stochează exemplarul master al fiecărei clase (și clasele sau actele fiică clasate în aceasta etc.); atunci când o asemenea schimbare este făcută, SMAE trebuie să mute conținutul din vechia poziție în noua poziție. *Această cerință este folositoare dacă se creează sau se elimină depozite sau dacă se mută acte într-un alt depozit, urmând mutările geografice determinate de funcțiile activității.*	D
10.10.16	Acolo unde SMAE acceptă depozite multiple, el trebuie să permită unui rol de administrator să adauge depozite.	D
10.10.17	Acolo unde SMAE acceptă multiple depozite, el trebuie să permită unui rol de administrator să elimine un depozit.	D

10.11 Activități offline și la distanță

Cerințele din această secțiune acoperă toate tipurile de utilizare mobilă și offline a SMAE de către utilizatori care nu sunt conectați în permanență la SMAE (sau la rețeaua care îl găzduiește).

Există câteva scenarii, care includ:

- utilizatori care au acces a SMAE folosind computere portabile (mobile, laptopuri, sau notebook-uri) sau PC care sunt conectate la rețea cu intermitență.
- utilizatori care se conectează la SMAE de la distanță, prin intermediul unei conexiuni prin apel telefonic sau prin orice altă conexiune cu bandă îngustă (de pildă, prin telecomutatoare sau dintr-un amplasament temporar).
- utilizatori are accesează SMAE folosind alte dispozitive mobile, cum ar fi PDA sau smartphone.

Computerele potabile pot fi folosite ca stații de lucru obișnuite atunci când sunt conectate la SMAE. Cu toate acestea, utilizatorii ar putea avea nevoie să descarce și să sincronizeze acte și date. astfel încât să lucreze cu ele în timp ce sunt deconectați.

Pentru a activa această funcționalitate, SMAE trebuie să descarce nu doar acte și alte grupări, ci de asemenea și metadatele lor. Va fi de asemenea nevoie ca SMAE să sincronizeze toate datele modificate atunci când utilizatorul va fi din nou conectat la sistem.

Într-o manieră similară, computerele portabile pot fi conectate intermitent la SMAE, de pildă când sunt folosite prin telecomutatoare. Atunci când sunt conectate, computerul portabil va trebui să se sincronizeze cu SMAE. Din nou va fi nevoie să se descarce acte etc., datele descărcate fiind administrate de computerul portabil în perioada dintre sincronizări.

PDA, smartphone-uri și alte dispozitive de mici dimensiuni pot fi folosite pentru a vizualiza și accesa actele, în multe cazuri folosind interfața unui program de parcurgere (*browser*). Limitări inerente, cum ar fi ecranul de mici dimensiuni și performanțele reduse, conduc la imposibilitatea, în multe cazuri, de a oferi o funcționalitate completă asemănătoare cu cea a unui computer portabil sau fix. Cu toate acestea, asemenea dispozitive sunt frecvent folosite pentru aplicații de e-mail mobil, notițe și calendar, și este prin urmare nevoie să se sincronizeze aceste tipuri de documente cu sistemul central.

MoReq2 nu precizează cerințe pentru a permite utilizatorilor mobili sau deconectați să gestioneze schema de clasificare (de pildă, crearea de noi clase) și dosarele (de pildă, închiderea unui dosar). Poate fi posibil să se dezvolte sisteme care acceptă o astfel de gestionare și MoReq2 nu împiedică acest lucru.

Ref	Cerință	Testabil
10.11.1	SMAE ar trebui să permită ca un rol de administrator să specifice grupările conținând informații care nu pot fi descărcate de orice utilizator. *Aceasta este o prevedere de securitate, pentru a proteja informațiile secrete de o eventuală descărcare și astfel de plasare a lor în afara controlului SMAE.*	D
10.11.2	SMAE trebuie să permită unui utilizator să descarce orice grupare sau acte însoțite de metadate, pentru ca utilizatorul să lucreze cu acestea în timp ce nu este conectat la rețea.	D

Ref	Cerință	Testabil
10.11.3	SMAE trebuie să înregistreze în evidența lui de auditare toate activitățile desfășurate asupra grupărilor, actelor și documentelor.	D
10.11.4	SMAE ar trebui să notifice în metadatele grupării, actului sau documentului că respectiva entitate a fost descărcată pentru utilizare offline.	P
10.11.5	SMAE trebuie să activeze sincronizarea documentelor, actelor și grupărilor descărcate în momentul conectării la sistem. *Aceasta înseamnă că el trebuie să actualizeze metadatele și să notifice utilizatorul pentru gestionarea conflictelor, dacă apare vreun conflict*	D
10.11.6	SMAE trebuie să actualizeze evidența de auditare cu informații asupra activității offline în momentul conectării la sistem.	D
10.11.7	SMAE trebuie să permită utilizatorului să captureze documentele create în timp ce era deconectat, apoi să le captureze ulterior ca acte, în momentul conectării la SMAE. *Dacă actele au fost create offline, atunci SMAE trebuie:* ▪ *fie să notifice utilizatorul, în momentul reconectării, prin dialogul de sincronizare, să le declare în clasa, dosarului, sub-dosarul sau volumul corespunzător.* ▪ *fie să le declare automat, în momentul reconectării, folosind clasa, dosarul, sub-dosarul sau volumul specificat de utilizator în perioada în care a fost deconectat (supusă validării).*	D
10.11.8	SMAE trebuie să aplice dispozitivelor conectate de la distanță toate restricțiile de acces și securitate. *SMAE nu trebuie să ofere nici o ocazie dispozitivelor portabile să încalce regulile de securitate ale SMAE. De pildă, un utilizator nu trebuie să poată descărca nici o informație la care el nu ar avea acces dacă ar fi online. Cu toate acestea, MoReq2 admite faptul că orice informație care a fost descărcată pe un dispozitiv nu se mai află sub controlul SMAE și că încălcarea securității în acest scenariu nu poate fi împiedicată de către SMAE.* *Următoarele 4 cerințe se aplică doar dacă SMAE acceptă managementul documentelor electronice, așa cum este definit în secțiunea 10.3. Se va folosi terminologia definită în acea secțiune.*	P
10.11.9	SMAE trebuie să permită unui utilizator să descarce documente cu metadatele care le însoțesc, pentru ca utilizatorul să lucreze cu acestea în timp ce este deconectat de la rețea.	D

Ref	Cerință	Testabil
10.11.10	SMAE trebuie să permită utilizatorilor opțiunea de verificare la ieșire a documentelor atunci când ele sunt descărcate.	D
10.11.11	Dacă un utilizator verifică la ieșire un document și lucrează cu acesta în timp ce nu este conectat la SMAE, sistemul trebuie să permită ca sistemul de numerotare al versiunilor să se aplice asupra documentului.	D
10.11.12	Dacă un utilizator verifică la ieșire un document și modifică numărul său de versiune în timp ce nu este conectat la un SMAE, atunci când utilizatorul se reconectează la SMAE acesta din urmă trebuie să permită utilizatorului să încarce documentul revizuit și trebuie ca în acel moment să îl verifice automat la intrare și să înregistreze modificările și numărul noii versiuni.	D

10.12. Integrarea faxului

Deși e-mail-ul a devenit predominant în majoritatea organizațiilor ca metodă preferată de comunicare rapidă, există însă unele situații și unele zone pentru care faxul este necesar.

O astfel de situație poate fi, de pildă, acolo unde documentul original nu este în format electronic și o copie trebuie transmisă unei alte organizații sau unde o reprezentare vizibilă (de pildă o semnătură) este necesară.

Anumite servere de fax se integrează cu sistemele de e-mail, astfel încât atât faxurile care sunt primite, cât și ce le care sunt expediate sunt tratate ca anexe ale mesajelor e-mail. În acest caz, cerințele din secțiunea 6.3 se aplică.

Acolo unde SMAE unei organizație este integrat cu un serviciu de faxuri se aplică următoarele cerințe.

Ref	Cerințe	Testabil
10.12.1	SMAE ar trebui să furnizeze o interfață de programare a aplicației (*application programming interface* — API) pentru a-i permite să relaționeze cu un server de fax.	N
10.12.2	SMAE trebuie să fie capabil să stocheze faxuri în formate standard, cum ar fi formatul de imagine TIFF v6 cu compresie Group IV. *Vezi ISO 12333 pentru implicațiile metodelor de compresie.*	D
10.12.3	EMS trebuie să accepte captura faxurilor de o manieră integrată, astfel încât captura să poată fi realizată de un utilizator din interfața pentru fax (dacă această există), fără ca utilizatorul să fie nevoit să comute la SMAE.	D

Ref	Cerințe	Testabil
10.12.4	SMAE trebuie să fie strâns integrat cu interfața de fax pentru a permite utilizatorilor să transmită prin fax orice act electronic din SMAE pe care îl vizualizează în acel moment sau cu care lucrează în SMAE (atât timp cât actul poate fi prezentat sub forma unei imagini bi-dimensionale).	D
10.12.5	Trebuie să fie posibil ca un rol de administrator să configureze SAME, astfel încât acesta să acționeze într-unul din următoarele moduri, atunci când utilizator al SMAE trimite un fax: ▪ capturează automat faxul ca act; ▪ notifică automat utilizatorul, dându-i acestuia posibilitatea de a declara faxul ca act. ▪ nu desfășoară nici o acțiune (și astfel se bazează pe utilizator că va iniția declararea, dacă este cazul). *Indiferent ce variantă este aleasă, se acceptă ca un SMAE să solicite utilizatorului să clasifice manual un act și să introducă manual metadatele.*	D
10.12.6	Trebuie să fie posibil ca un rol de administrator să configureze SMAE astfel încât acesta să acționeze într-unul din următoarele moduri, atunci când utilizator al SMAE primește un fax: ▪ notifică automat utilizatorul, dându-i acestuia posibilitatea de a declara faxul ca act. ▪ nu desfășoară nici o acțiune (și astfel se bazează pe utilizator că va iniția declararea, dacă este cazul). *Indiferent ce variantă este aleasă, se acceptă ca un SMAE să solicite utilizatorului să clasifice manual un act și să introducă manual metadatele.*	D
10.12.7	SMAE ar trebui să fie capabil să extragă automat elementele de metadate ale faxului din faxurile primite, așa cum se precizează în capitolul 12, de pildă: ▪ Titlul; ▪ Emitent; ▪ Data și ora; ▪ Destinatar. *Aceasta poate fi îndeplinită prin intermediul unui șablon de fax și este relevant doar acolo unde faxurile au o structură internă predictibilă.*	D

Ref	Cerințe	Testabil
10.12.8	SMAE ar trebui să fie capabil să introducă automat elementele de metadate ale faxului pentru faxurile expediate, așa cum se precizează în capitolul 12, de pildă: ▪ Titlul; ▪ Emitent; ▪ Data și ora; ▪ Destinatar. *Aceasta poate fi îndeplinită prin intermediul unui șablon de fax și este relevant doar acolo unde faxurile au o structură internă predictibilă.*	D
10.12.9	SMAE trebuie să permită unui utilizator care capturează un fax să editeze elementul de metadată Titlu, pentru a reflecta conținutul faxului.	D
10.12.10	SMAE ar trebui să poată furniza un gen de act fax, atât pentru faxurile primite, cât și pentru cele emise, pentru a permite utilizatorului să introducă metadate.	D

10.13. Categorii de securitate

Capitolul 4 descrie cerințele pentru a controla accesul rolurilor şi grupurilor la grupări şi acte. În anumite medii, cum ar fi cele implicând securitatea naţională, sistemul medical etc., există o nevoie suplimentară de a limita accesul, folosind un sistem de categorii de securitate şi autorizații de securitate.

Aceste autorizații prevalează asupra oricărui alt drept de acces care ar putea fi acordat folosind caracteristicile definite în capitolul 4. Cerinţele din această secţiune se aplică doar pentru organizaţiile care au asemenea nevoi.

Implementarea sistemului se realizează prin alocarea pentru clase, dosare, sub-dosare, volume şi/sau acte a uneia sau mai multor ,,categorii de securitate".

Termenul ,,categorii de securitate" este folosit în această specificaţie cu sensul ,,unul sau mai mulţi termeni asociaţi cu un act, care definesc regulile ce guvernează accesul la ele". De remarcat că acest termen este folosit special pentru această specificare şi nu este o întrebuinţare generală.

Utilizatorilor li se poate aloca o singură autorizație de securitate, care împiedică accesul la toate grupările sau actele căror le-au fost atribuite categorii de securitate mai mari.

Categoriile de securitate pot fi compuse din sub-categorii. Unele sub-categorii sunt ierarhice prin natura lor. Altele pot fi ordonate diferit, în mod obişnuit de o manieră care este unică unei organizaţii sau unui sector.

MoReq2 descrie în detaliu doar cerinţele pentru sub-categorii ierarhice.

Exemplele furnizate aici se bazează pe marcajele din domeniul siguranţei naţionale, dar aceleaşi principii se aplică şi marcajelor din alte sectoare.

Pot exista de asemenea şi cerinţe de clasificare de siguranţă naţională specifice fiecărei ţări. Acolo unde este cazul, acestea pot fi tratate în capitolul zero.

Ref	Cerință	Testabil
10.13.1	SMAE trebuie să permită ca una din următoarele opţiuni să fie selectate în momentul configurării sistemului. ▪ categoriile de securitate sunt atribuite claselor, dosarelor, sub-dosarelor şi/sau volumelor (şi nu actelor individuale); ▪ categoriile de securitate sunt atribuite actelor individuale (şi nu claselor, dosarelor, sub-dosarelor şi/sau volumelor); ▪ categoriile de securitate sunt atribuite atât actelor individuale, cât şi claselor, dosarelor, sub-dosarelor şi/sau volumelor. *Unele organizaţii vor dori să controleze acte secrete la nivel individual, în timp ce altele vor dori să le controleze la nivel de clasă, dosar etc.*	D
10.13.2	SMAE trebuie să permită unui rol de administrator să specifice, în momentul configurării sistemului, ce rol poate specifica şi schimba categoriile de securitate ale actelor şi grupărilor. *În unele organizaţii, doar responsabilii informaţiilor pot avea acest privilegiu. În altele, diferite roluri, cum ar fi cel al revizorului de securitate ori al administratorului de activitate (dacă asemenea roluri există) vor avea aceste privilegii.*	D
10.13.3	SMAE trebuie să permită, deşi nu este obligatoriu, ca o categorie de securitate să fie alcătuită din mai multe „sub-categorii”. *De pildă, o categorie de securitate poate fi alcătuită din 3 sub-categorii, ca în următorul exemplu imaginar:* ▪ *Clasa de securitate;* ▪ *Atenţionare* ▪ *Descriptor.* *Fiecare sub-categorie poate fi gândită ca una dintre dimensiunile care definesc securitatea informaţiei. Deci, în acest exemplu, orice combinaţie validă a celor 3 sub-categorii de securitate clasă, avertisment şi descriptor poate fi aplicată unui act.*	D
10.13.4	SMAE trebuie să ceară ca rolul de utilizator să definească şi să întreţină vocabulare controlate, aceste vocabulare limitând valorile permise pentru fiecare sub-categorie.	D

Ref	Cerință	Testabil

De exemplu, nivelurile pot exista ca în următorul exemplu imaginar:

Sub-categorie	***Valori disponibile***
Clasă	*Strict secret de importanţă deosebită*
	Strict secret
	Secret
	Secret de serviciu
	Nesecret
Atenţionare	*Doar pentru NATO*
	Doar pentru Vestul Europei
Descriptor	*Comercial*
	Personal
	Management
	Audit şi contabilitate

În acest exemplu imaginar, sub-categoria „clasa de securitate" este ierarhică (vezi 10.13.6), în timp ce alte sub-categorii nu. Cerinţele pentru sub-categorii ierarhice sunt obişnuite şi sunt specificate mai jos.

Cerinţele pentru sub-categoriile non-ierarhice pot fi complexe şi sunt specifice sectorului în care ele sunt implementate; cu excepţia cerinţelor 10.13.5 şi 10.13.7, acestea nu sunt detaliate aici.

10.13.5 SMAE ar trebui să permită implementări specifice ale regulilor de securitate unice sau complexe. N

Acestea pot fi realizate prin interfeţe corespunzătoare de programe. Exemple ale acestei necesităţi includ nevoia de a administra actele folosind convenţii de marcare ce nu sunt prezentate aici, cum ar fi marcajele IDO (International Defence Organisation — Organizaţia internaţională de apărare) sau restricţii de acces pentru actele medicale.

10.13.6 Pentru cel puţin o sub-categorie, SMAE trebuie să accepte o ierarhie de cel puţin 5 niveluri, de la acces nerestricţionat la cel mai înalt nivel până la cel mai restricţionat acces la cel mai mic nivel. D

Sub-categoria ,,clasa de securitate" din cerinţa 10.13.3 este un exemplu în acest sens.

Ref	Cerință	Testabil
10.13.7	Acolo unde o sub-categorie şi autorizațiile corespunzătoare nu sunt ierarhice, SMAE trebuie să permită ca una din următoarele opţiuni să fie selectate în momentul configurării sistemului: ▪ SMAE trebuie să solicite ca o autorizație valabilă să fie introdusă pentru fiecare nou utilizator. ▪ SMAE trebuie să aplice o autorizație predefinită pentru noii utilizatori. Un rol de administrator trebuie să fie capabil să redefinească autorizația predefinită în momentul configurării sistemului sau în orice alt moment. *Cu alte cuvinte, autorizațiile trebuie să fie obligatorii pentru utilizatori.*	D
10.13.8	Acolo unde SMAE aplică noilor utilizatori o autorizație predefinită organizată ierarhic (ca în cerinţa 10.13.7), el trebuie să aplice o autorizație predefinită pentru noii utilizatori care reprezintă cel mai scăzut nivel de autorizare din ierarhie (adică, cel mai restrictiv).	D
10.13.9	SMAE trebuie să rezerve accesul la acte (și la clase, dosare, sub-dosare şi volume, în funcţie de selectarea făcută pentru 10.13.1) pentru acei utilizatori care au o autorizație de securitate egală cu sau mai mare decât categoria de securitate. *De remarcat că această autorizație poate să nu fie suficientă pentru a obţine accesul. Accesul la actele electronice poate fi rezervat suplimentar doar pentru anumiţi utilizatori, roluri şi/sau grupuri, folosind caracteristicile descrise în capitolul 4.*	D
10.13.10	Acolo unde o sub-categorie este ierarhică, SMAE trebuie sa folosească unul din următoarele moduri de acțiune pentru a atribui o sub-categorie unor noi clase, acte etc., ce pot fi selectate de către un rol de administrator în momentul configurării sistemului sau la orice moment ulterior: ▪ SMAE trebuie să aplice o valoare predefinită care este selectată de un rol de administrator; ▪ SMAE trebuie să folosească valoarea grupării mamă ca predefinită; ▪ SMAE trebuie să ceară unui rol de administrator să introducă o valoare.	D

Ref	Cerință	Testabil
10.13.11	Acolo unde o sub-categorie nu este ierarhică, SMAE trebuie să folosească unul din următoarele moduri de operare pentru a atribui o sub-categorie unei noi clase, acte etc., ce poate fi selectată de către un rol de administrator în momentul configurării sistemului sau la orice moment ulterior: ▪ SMAE trebuie să aplice o valoare predefinită care este selectată de un rol de administrator; ▪ SMAE trebuie să folosească valoarea grupării mamă ca predefinită; ▪ SMAE trebuie să permită, dar nu să ceară, unui rol de administrator să introducă o valoare.	D
10.13.12	Atunci când o nouă categorie sau sub-categorie ierarhică de securitate este definită, SMAE trebuie să aplice valoarea predefinită pentru toate clasele, actele etc. existente, care este cel mai mic nivel din ierarhie; cu alte cuvinte, valoarea predefinită acordă cel mai mic nivel de acces permis de ierarhie.	D
10.13.13	SMAE ar trebui să permită ca autorizațiile de securitate să fie alocate unui rol şi să fie moştenite de utilizatori. Acolo unde o autorizație de securitate este moştenită dintr-un rol, SMAE trebuie să permită ca o autorizație de securitate diferită să fie aplicată la nivel de utilizator individual.	D
10.13.14	Dacă SMAE accepta categorii de securitate atât pentru acte cât şi pentru clase etc. (vezi 10.13.1), atunci el trebuie să fie capabil să împiedice ca o clasă, dosar, sub-dosar sau volum să aibă o categorie de securitate mai mică decât un act cuprins în acestea.	D
10.13.15	Dacă un utilizator încearcă să captureze un act care are o categorie mai înaltă de securitate decât gruparea în care este capturat, SMAE trebuie să notifice utilizatorului, astfel încât măsurile corespunzătoare să fie luate; SMAE trebuie să permită cel puţin următoarele acţiuni (condiţionate de activarea lor în momentul configurării sistemului): ▪ categoria de securitate a grupării este ridicată la cea a actului; ▪ utilizatorului i se refuza permisiunea de a captura actul în grupare; ▪ actul este în mod automat transmis unui utilizator precizat pentru acţiunea corespunzătoare; Utilizatorul este invitat să creeze o nouă grupare pentru act, cu valori predefinite ale metadatelor preluate din gruparea iniţială, într-un singur proces integrat.	D

Ref	Cerință	Testabil
10.13.16	Un rol de administrator trebuie să poată stabili cea mai înaltă categorie de securitate a oricărui act din orice clasă, dosar, sub-dosar sau volum printr-o simplă interogare. *În anumite medii, aceasta va fi o caracteristică importantă în sprijinul administrării.*	D
10.13.17	Condiţionat de îndeplinirea cerinţei 10.13.1, un rol de administrator trebuie să poată schimba categoria de securitate a unei clase, dosar, sub-dosar, volum sau act. *Vezi şi 10.13.27.*	D
10.13.18	SMAE trebuie să accepte revizuiri ale categoriilor de securitate de o manieră periodică, rutinieră şi programată, unde o revizuire constă din: ▪ a permite unui utilizator (cu autorizația și permisiunile corespunzătoare) să vizualizeze actele specificate şi categoriile lor de securitate. ▪ a permite utilizatorului să modifice categoriile de securitate. *MoReq2 nu precizează cum trebuie să fie realizată această cerinţă.*	D
10.13.19	SMAE trebuie să reţină automat un istoric al valorilor categoriei de securitate în metadatele actelor, claselor etc. cărora li se aplică.	D
10.13.20	Atunci când un utilizator modifică valoarea unei categorii de securitate (fie în timpul revizuirii, ca la 10.13.18, fie cu altă ocazie), SMAE trebuie să permită utilizatorului să introducă motivaţia schimbării şi trebuie să stocheze acest motiv cu istoricul său (ca la 10.13.19) ca metadate. *Vezi 10.13.2 pentru detalii asupra utilizatorilor ce au autorizație de a schimba categoriile de securitate.*	D
10.13.21	SMAE trebuie să permită utilizatorilor care deţin aprobări care le îngăduie să vadă un act, să vadă valoarea actuală a categoriei(iilor) de securitate şi orice istoric al acestor valori (ca în 10.13.19).	D
10.13.22	SMAE ar trebui să accepte alocarea de categorii de securitate unei clase, dosar, sub-dosar sau volum, care sunt valabile pentru o anumită perioadă de timp şi la sfârşitul respectivei perioade ar trebui să retrogradeze automat marcajul la cel mai scăzut nivel de securitate.	D

Ref	Cerință	Testabil
10.13.23	SMAE ar trebui să accepte alocarea de categorii de securitate unei clase, dosar, sub-dosar sau volum, care sunt valabile pentru o anumită perioadă de timp şi ar trebui să retrogradeze automat marcajul la un nivel de securitate inferior, pre-selectat, la sfârşitul respectivei perioade.	D
10.13.24	SMAE ar trebui să accepte notificarea unui rol de administrator la expirarea perioadei de timp specificate pentru care o categorie de securitate a fost atribuită unei clase, dosar, sub-dosar sau volum şi să permită ca marcajele de securitate să fie reevaluate şi modificate. *De pildă, SMAE ar trebui să transmită o informaţie la ,,Data naşterii + X ani". Acest exemplu se poate folosi pentru actele medicale sau pentru alte scopuri prevăzute în legea de protecţie a datelor personale.*	D
10.13.25	SMAE trebuie să înregistreze automat în evidenţa de auditare toate schimbările făcute asupra valorilor categoriilor şi subcategoriilor de securitate.	D
10.13.26	SMAE trebuie să nu permită unui utilizator să aplice o categorie de securitate unei clase, dosar, sub-dosar sau volum la care utilizatorul nu are acces.	D
10.13.27	Un rol de administrator trebuie să poată modifica categoria de securitate a tuturor actelor şi a entităţilor subordonate (condiţionate de opţiunile configurare la 10.13.1) dintr-o clasă, dosar, sub-dosar sau volum printr-o singură acțiune. *Aceasta este cerută în mod periodic pentru a reduce nivelul de protecţie atribuit actelor pe măsură ce gradul de importanţă al secretului scade în timp.*	D
10.13.28	SMAE trebuie să furnizeze un avertisment către rolul de administrator dacă vreunui act i se scade categoria de securitate şi să aştepte confirmarea înainte de finalizarea acţiunii. *Această cerință este în mod special de ajutor dacă o categorie de securitate a unei grupări este coborâtă sub nivelul actelor care sunt stocate în ea.*	D
10.13.29	SMAE trebuie să înregistreze automat istoricul (de pildă, datele şi detaliile oricărei modificări ale categoriilor de securitate) în metadatele clasei, dosarului, sub-dosarului, volumului şi actului relevant. *Istoricul trebuie să includă, pentru fiecare schimbare efectuată, data, utilizatorul valorile înainte şi după modificare şi motivul.*	D

11. Cerinţe non-funcţionale

Unele din atribuţiile unei implementări de succes a unui SMAE nu poate fi definită în termeni de funcţionalitate. În practică, cerinţele non-funcţionale sunt importante pentru succes. Acest capitol strânge laolaltă aceste cerinţe.

Secţiunile din acest capitol listează cerinţele pentru următoarele zone:

- Uşurinţa în folosire (secţiunea 11.1)
- Performanţă şi scalabilitate (secţiunea 11.2)
- Disponibilitatea sistemului (Secţiunea 11.3)
- Standarde tehnice (secţiunea 11.4);
- Mediul legislativ şi de reglementare (secţiunea 11.5);
- Externalizare şi administrarea datelor de către terţi (secţiunea 11.6)
- Prezervarea şi învechirea tehnologică (secţiunea 11.7)
- Procesele de activitate (secţiunea 11.8).

Aceste cerinţe non-funcţionale sunt adesea dificil de definit şi dificil de măsurat obiectiv. Cu toate aceste este important să fie identificate, astfel încât acestea să poată fi luate în considerare, cel puţin în linii generale. Unele sunt specifice EDRM, dar câteva sunt generice mai multor feluri de sisteme IT.

Ca o adăugare la acest capitol, utilizatorii acestei specificaţii vor trebui să ia în considerare nevoile organizaţiei în legătură cu standardele actuale tehnice şi operaţionale. Vor trebui să ia în considerare, de asemenea, şi serviciile de sprijin pe care le oferă furnizorul SMAE, incluzând documentaţia, personalizare, pregătirea şi consultanţa.

Organizaţiile vor trebui să adauge propriile lor cerinţe în aceste zone, în funcţie de mărimea şi structura lor, de caracteristicile fizice şi mediul actual de operare tehnică. Această secţiune este destinată ca o listă de control a aspectelor pe care utilizatorii vor trebui să le ia în considerare. Aceste cerinţe specifice vor trebui să fie adăugate cerinţelor generale descrise în secţiunile anterioare.

Unele din cerinţele exemplu din acest capitol folosesc paranteze unghiulare pentru a indica faptul că un utilizator al specificaţiilor trebuie să introducă o valoare cuantificabilă sau alte informaţii specifice aplicaţiilor. De pildă,

<xx minute/ore>

înseamnă că un utilizator al specificaţiei ar trebui să introducă durata de timp, probabil măsurată în minute sau ore, pentru a corespunde cerinţei specifice.

În mod similar,

<4 secunde>

înseamnă că utilizatorul specificaţiei ar trebui să specifice un interval de timp; 4 secunde este sugerat aici ca un exemplu de pornire.

Într-un mod similar, expresiile alternative sunt de asemenea găsite în paranteze unghiulare. De exemplu, expresia:

<în fiecare zi/în toate zilele săptămânii/xx zile pe an>

ar trebui înţelese cu semnificaţia: „în fiecare zi sau în fiecare zi a săptămânii sau într-un număr precizat de zile pe an sau asemănător”, după cum este potrivit pentru organizaţie.

În toate cazurile, „xx” înseamnă număr, indiferent de valoare.

Datorită faptului că cerinţele sunt generale, şi deoarece diferite organizaţii vor avea cerinţe şi priorităţi extrem de diferite, cerinţele non-funcţionale din acest capitol nu sunt testate în Cadrul de testare MoReq2. Atributele testabile care sunt precizate aici sunt destinate folosirii ca linii directoare. Organizaţiile şi utilizatorii MoReq2 vor fi nevoiţi să analizeze cerinţele lor, să îşi stabilească priorităţile şi să realizeze propriile lor teste în aceste zone.

11.1 Uşurinţa în folosire

Atunci când se iau în considerare cerinţele non-funcţionale în dezvoltarea specificaţiei unui SMAE, acestea trebuie să includă gradul cerut de uşurinţă în folosire şi cum trebuie aceasta să fie specificat. Aceasta va depinde de tipul utilizatorilor cărora sistemul le este destinat şi amploarea pregătirii pe care vor trebui să o desfăşoare. Exemple de cerinţe pentru uşurinţa în folosire sunt listate mai jos.

Ref	Cerinţe exemplu	Testabil
11.1.1.	SMAE trebuie să permită unui rol de administrator să configureze cât anume din schema de clasificare poate fi accesată de către fiecare rol de utilizator sau grup de utilizatori. *De exemplu, un utilizator sau un grup de utilizatori, de pildă, lucrători de caz, poate fi limitat la vizualizarea unei singure clase din schema de clasificare sau chiar la a unui dosar sau sub-dosar.*	D
11.1.2.	SMAE trebuie să furnizeze asistenţă online în cadrul întregului sistem	D
11.1.3.	SMAE trebuie să reprezinte grafic schema de clasificare în mod ierarhic şi să permită utilizatorilor să navigheze în cadrul ei folosind reprezentarea grafică.	D
11.1.4.	Asistenţa online din SMAE trebuie să fie contextuală.	D

Ref	Cerinţe exemplu	Testabil
11.1.5.	SMAE ar trebui să includă asistenţă privind folosirea schemei de clasificare, incluzând, cel puţin, acces simplificat la metadatele descriptive pentru clase, dosare, sub-dosare şi volume.	P
11.1.6.	SMAE ar trebui să cuprindă un tezaur care să asiste utilizatorii în selectarea termenilor pentru cuvinte-cheie, descrieri etc. *Vezi 11.4.1, 11.4.2 şi 11.8.11.*	D
11.1.7.	Toate mesajele de eroare produse de un SMAE trebuie să fie inteligibile, astfel încât utilizatorii să poată decide cum să corecteze erorile sau să anuleze procesul. *La modul ideal, fiecare mesaj de eroare va fi însoțit de un text explicativ, și de o indicație a acțiunilor pe care un utilizator le poate lua ca răspuns la respectiva eroare.*	N
11.1.8.	Interfața SMAE cu utilizatorul ar trebui să fie potrivită pentru utilizatori cu cea mai largă paletă de nevoi și abilități. Aceasta înseamnă că trebuie să fie proiectată în conformitate cu liniile directoare și standardele de accesibilitate corespunzătoare și compatibilă cu aplicațiile obișnuite specializate în accesibilitate. *Vezi anexa 7 pentru liniile directoare și standardele corespunzătoare.*	N
11.1.9.	Documentația SMAE ar trebui să fie furnizată într-un format util, astfel încât utilizatorii cu o mare diversitate de nevoi și abilități să o poată folosi. *Vezi anexa 7 pentru liniile directoare și standardele corespunzătoare.*	N
11.1.10.	SMAE trebuie să fie ușor de folosit și intuitiv. *Ușurința în folosire poate fi evaluată de un grup de utilizatori obișnuiți.*	N
11.1.11.	Regulile și comportamentul interfeței pentru utilizator a unui SMAE trebuie să fie consecventă în toate aspectele sistemului, incluzând ferestre, meniuri și comenzi. Acestea trebuie să fie de asemenea consecvente cu mediul sistemului de operare în care operează SMAE. *Regulile ar trebui să fie consecvente cu alte aplicații de bază deja instalate.*	P
11.1.12.	SMAE trebuie să poată afișa simultan, mai multe acte și grupări.	D
11.1.13.	SMAE trebuie să accepte o interfață grafică cu utilizatorul.	D

Ref	Cerinţe exemplu	Testabil
11.1.14.	SMAE trebuie să permit utilizatorilor să mute, redimensioneze și să modifice aspectul ferestrelor și să salveze modificările în profilul său de utilizator, astfel încât acestea să se încarce automat atunci când utilizatorul se loghează la SMAE.	D
11.1.15.	SMAE trebuie să permit utilizatorilor să personalizeze aspectele interfeței grafice pentru utilizator. Personalizarea ar trebui să includă, fără a se limita, următoarele modificări: ▪ meniul și conținutul barelor de instrumente; ▪ amplasarea ecranului; ▪ folosirea tastelor funcționale; ▪ culorile ecranului, fonturile și mărimea acestora.; ▪ alertele sonore.	D
11.1.16.	SMAE ar trebui să permită utilizatorilor să selecteze sunete și volumul alertelor și să salveze modificările în profilul de utilizator.	D
11.1.17.	SMAE trebuie să permită valori implicite repetate pentru introducerile de date, acolo unde se dorește. Aceste valori implicite ar trebui să includă: ▪ valori definite de utilizator; ▪ o valoare implicit fixă; ▪ valoare similară celei anterioare; ▪ valori derivate din context, de pildă data curentă, numărul dosarului, identificatorul utilizatorului; ▪ alte valori corespunzătoare.	P
11.1.18.	SMAE trebuie să permită meniuri configurabile tip meniu ascuns (*drop-down*) sau listă de opțiuni (*pick list*) pentru valorile elementelor de metadate pentru intrările de date. *Conținutul acestor liste trebuie să fie configurabil de către administrator.*	D
11.1.19.	Tranzacțiile frecvent executate ale SMAE trebuie să fie proiectate astfel încât ele să poată fi realizate cu un număr mic de interacțiuni (de pildă, apăsări pe mouse sau apăsări pe tastatură).	P
11.1.20.	SMAE trebuie să fie strâns integrat cu sistemul de e-mail al organizației, astfel încât să permită utilizatorilor să trimită acte și grupări de o manieră electronică, fără a părăsi SMAE.	N

Ref	Cerinţe exemplu	Testabil
	De exemplu, utilizatorul ar trebui să poată trimite din clientul de e-mail al SMAE. Esența acestei cerințe este că utilizatorul nu trebuie să comute în aplicația de e-mail pentru a trimite un act.	
11.1.21.	Acolo unde cerința 11.1.20 se aplică, SMAE ar trebui să o satisfacă prin transmiterea de indicatori (*pointer*) sau legături către grupări și acte și nu prin trimiterea de copii, ori de câte ori o grupare sau un act sunt trimise unui alt utilizator al SMAE. *Pot exista excepții la această cerință, de pildă, un utilizator de la distanță care nu are acces continuu la depozitul central.*	N
11.1.22.	SMAE ar trebui să indice dacă un mesaj e-mail are vreo anexă. *De exemplu, prin intermediul unei iconițe.*	D
11.1.23.	SMAE ar trebui să accepte funcții programabile de către utilizator. *De pildă, macro-comenzi ce pot fi definite de utilizator.*	D
11.1.24.	Atunci când utilizatorii trebuie să introducă metadate din acte care sunt imagini ale documentelor imprimate (de ex. imagini scanate), SMAE ar trebui să furnizeze caracteristici care să permită folosirea recunoașterii optice de caractere pentru a captura metadatele din imagine (recunoaștere zonală optică a caracterelor) *De pildă, utilizatorul ar trebui să poată selecta un spațiu din imagine care conține metadate, cum ar fi data sau titlul, și apoi să convertească acea imagine în valori de metadate și să le insereze în elementul de metadată dorit, totul dintr-o singură acțiune.*	D
11.1.25.	SMAE ar trebui să permit utilizatorilor să definească referințe încrucișate între actele înrudite, atât în cadrul aceleiași grupări, cât și din grupări diferite, permițând navigarea ușoară între acte.	D
11.1.26.	Atunci când un act sau o grupare (clasă, dosar, sub-dosar sau volum) de acte este vizualizată sau este în lucru, ca rezultat al căutării sau nu, un utilizator ar trebui să folosească caracteristicile SMAE pentru a regăsi informația despre următorul nivel ierarhic superior de grupare a actelor de o manieră simplă și fără să părăsească sau să închidă actul. *De exemplu, atunci când este citit un act, utilizatorul ar trebui să poată identifica în ce clasă, dosar, sub-dosar sau volum se află; dacă se vizualizează metadatele dosarului, utilizatorul ar trebui să poată să regăsi informații despre clasa în care este localizat.*	D

Ref	Cerinţe exemplu	Testabil
11.1.27.	SMAE ar trebui să permită unui utilizator care are acces la un dosar sau act să verifice dacă un alt utilizator, grup sau rol specificat are acces la el. *Aceasta cerință este prezentă pentru a permite utilizatorilor să indice explicit un utilizator, grup sau rol. Astfel, un utilizator poate interoga despre drepturile altui utilizator, în contextul unui act sau al unui dosar, fără a avea nevoie să cunoască grupul acelui utilizator sau apartenența la un anume rol.*	D
11.1.28.	SMAE ar trebui să permită unui utilizator să reducă riscul ce poate apare ca urmare a unei erori de clasificare a unui act, prin permisiunea acordată utilizatorilor de a aplica o blocare temporară a actului sau dosarului, printr-o singură apăsare. Această blocare temporară ar trebui să împiedice accesul la acel dosar sau la acel act pentru toți utilizatorii, cu excepția rolurilor de administrator; și SMAE ar trebui să informeze în mod automat rolul de administrator că o blocare temporară a fost aplicată, permițând astfel rolului de adminsitrator (și doar acestuia) să înlăture blocarea temporară. *Aceasta cerință este prezentă pentru a permite utilizatorilor să corecteze o eroare — cum ar fi plasarea accidentală a unui act secret într-un dosar nesecurizat, de pildă, ca rezultat al tehnicii „trage și plasează”* (*drag and drop*). *Deoarece utilizatorii nu au permisiunea de a șterge, înlătura sau modifica acte, aceasta cerință implică o acțiune a administratorului.* *Pentru a preveni utilizarea greșită a acestei facilități, este important ca utilizatorilor să le fie furnizate linii directoare pentru folosirea blocării temporare și ca rolurile de administrator să certifice ca aceasta să nu fi folosită abuziv.*	D
11.1.29.	Utilizatorii ar trebui să fie capabili să copieze acte din SMAE în orice alte medii de lucru, cum ar fi într-un dosar pe suprafața de lucru (*desktop*), folosind tehnica de ,,trage și plasează”, fără ca această acțiune să producă vreo schimbare asupra actului sau a metadatelor sale. *Atunci când o copie a unui act este plasată în orice alt mediu, este acceptabil ca acesta să își piardă metadatele (pe principiul că cele mai multe alte medii nu acceptă modelul de metadate MoReq2).*	P
11.1.30.	SMAE ar trebui să furnizeze asistență care să furnizeze o ghidare vizuală. *De pildă, includerea capturilor de ecran și/sau animațiilor care să arate utilizatorilor cum să folosească caracteristice sistemului.*	P
11.1.31.	SMAE ar trebui să permit utilizatorilor să marcheze zonele de asistență a sistemului ca zone favorite sau cu un sistem asemănător, astfel încât să le poată regăsi cu ușurință cu o ocazie viitoare.	D

Ref	Cerinţe exemplu	Testabil
11.1.32.	Un utilizator care lucrează cu un dosar trebuie să fie capabil să descopere ușor și rapid cuvintele cheie asociate cu acel dosar. *Trebuie să fie posibil să descopere cuvintele-cheie fără a fi nevoit să părăsească dosarul, într-o manieră care permite ca activitatea cu dosarul să continue fără întrerupere.*	D
11.1.33.	SMAE ar trebui să permită utilizatorilor să își definească clase, dosare și acte ca scurtături ,,favorite", astfel încât să le poată găsi ușor intr-o ocazie viitoare.	D
11.1.34.	SMAE ar trebui să permită utilizatorilor să transmită scurtăturile favorite altor utilizatori. *Favoritele pot fi remise prin e-mail sau prin alt mecanism.*	D

11.2 Performanță și scalabilitate

Utilizatorii acestei specificații ar trebui să ia în considerare amploarea până la care SMAE furnizează răspunsuri în timp util raportat la așteptările utilizatorilor, și dacă este capabil să deservească întregul număr de utilizatori pentru care este intenționat. Câteva considerații și cerințe exemplu sunt furnizate mai jos.

Timpul de răspuns întâmpinat de utilizatori va depinde de asemenea de alți factori, exteriori unui SMAE, incluzând:

- lățimea de banda a rețelei;
- încărcarea rețelei;
- timpul de așteptare al rețelei;
- configurarea și utilizarea diferitelor resurse de servere.

Prezenta specificație nu poate trata asemenea factori externi, dincolo de a releva că ei nu trebuie ignorați. In mod obișnuit, testarea în teren este necesară pentru a obține o perspectivă de încredere asupra performanței.

În mod similar, aceste cerințe ar trebui să fie interpretate cu o înțelegere standardizată a ceea ce înseamnă ,,timp de răspuns". Această înțelegere va varia de la mediu la mediu, în funcție de situația infrastructurii.

De exemplu, dacă un SMAE este destinat pentru o infrastructura existentă, este potrivit să se precizeze timpul de răspuns în termeni de perioadă de timp între primirea unei apăsări de taste la server și trimiterea răspunsului; sau, dacă SMAE este destinat pentru o nouă rețea, ar fi mai potrivit să se precizeze timpul de răspuns în termeni de perioadă de timp între introducerea unei cerințe la stația de lucru și primirea răspunsului la stația de lucru.

Cerințe specifice pentru activitatea offline și de la distanță sunt tratate în secțiunea 10.11 și aceste cerințe exemplu vor trebui modificate corespunzător pentru aceste medii.

SMAE trebuie să își poată desfășura toate funcțiile și să opereze uniform pentru a îndeplini nevoile utilizatorilor și activității, așa cum este definit în cerințele exemplu de mai jos.

Ref	Cerințe exemplu	Testabil
11.2.1	SMAE trebuie să furnizeze timpi de răspuns adecvați pentru a satisface nevoile activității pentru funcțiile desfășurate în mod obișnuit, în condiții standard, ca de exemplu: ▪ <100%> din totalul anticipat al utilizatorilor sunt logați și activi; ▪ <100%> din cantitatea totală anticipată a documentelor este administrată de sistem ▪ utilizatorii desfășoară o combinație obișnuită de tipuri de tranzacții la diferite intensități; ▪ constanța performanței pentru cel puțin 10 încercări de a realiza tranzacțiile	N
11.2.2	SMAE trebuie să poată returna rezultatele unei simple căutări (lista de regăsiri) într-un interval de <3 secunde> și pentru o căutare complexă (combinând 4 termeni) într-un interval de <10 secunde>, indiferent de capacitatea de stocare sau numărul de acte și dosare din sistem. *În acest context, desfășurarea unei căutări înseamnă returnarea unei liste de regăsiri (vezi 8.2.10). Nu include regăsirea actelor în sine.*	N
11.2.3	SMAE trebuie să poată regăsi și afișa într-un interval de <4 secunde> prima pagină a actului care a fost accesat într-un interval anterior de <xx> luni, indiferent de capacitatea de stocare sau numărul de acte și dosare din sistem. *Această cerință și cea de la 11.2.4, se aplică doar documentelor care pot fi prezentate sub forma paginilor. Dacă documentele sunt neobișnuit de ample, poate fi necesar să se mărească timpul acceptabil de răspuns.* *Includerea formulării ,,în cadrul a <xx> luni anterioare"implică folosirea unui dispozitiv de stocare fizică „*staged*" sau ierarhic. Vezi de asemenea și cerința următoare.* *Această cerință urmărește să permită regăsirea rapidă a actelor cu utilizare frecventă, pe baza premizei că frecvența utilizării este în mod obișnuit corelată cu folosirea recentă. Perioada de timp trebuie introdusă de organizație, pe baza evaluării timpului după care scade rata de folosire frecventă a actelor.*	N

Ref	Cerințe exemplu	Testabil
11.2.4	SMAE trebuie să poată regăsi și afișa într-un interval de <20 de secunde> prima pagină a unui act care nu a fost accesat în anterioarele <xx> luni, indiferent de capacitatea de stocare sau numărul de acte și dosare din sistem. *Această cerință urmărește să permită existența cazurilor când este folosită o formă a managementului de stocare ierarhic, când actele folosite cu o frecvență redusă sunt stocate pe medii mai puțin rapide ca actele mai frecvent folosite, sau sunt stocate în apropierea rețelei (near line). Perioadele de timp trebuie să fie precizate de organizație, pe baza evaluării timpului după care scade rata de folosire frecventă a actelor.* *Atât pentru această cerință, cât și pentru cea precedentă, dacă toate actele electronice sunt stocate folosind un singur dispozitiv fizic (de pildă, fără dispozitive de stocare ierarhice sau staged), atunci formularea „în cadrul anterioarelor <xx>luni"este irelevantă și ar trebui eliminată.*	N
11.2.5	SMAE trebuie să permit o singură implementare a sistemului pentru a avea o stocare de acte electronice de cel puțin <xx GB/TB/PB> sau <XX mii, milioane/miliarde> acte, și pentru a deservi cel puțin <XX sute/mii> utilizatori simultan, cu nivelurile de performanță specificate în această secțiune. *Estimările privind cerințele de stocare și numărul de acte și de utilizatori trebuie introduse de organizație. A se observa că în organizațiile de amploare, se pot acumula cantități mari de acte — în unele cazuri se poate ajunge la miliarde de acte.*	N
11.2.6	SMAE trebuie să furnizeze nivelurile de performanță specificate în această secțiune cu cantități de până la, cel puțin: ▪ <*xx*> clase; ▪ <*xx*> dosare per clasă; ▪ <*xx*> sub-dosare per dosar; ▪ <*xx*> volume per sub-dosar; ▪ <*xx*> acte per volume. *Acestea sunt unități de măsură cu rol orientativ. Organizațiile ar trebui să ia în considerare dacă alte unități de măsură similare se aplică contextului lor.*	N
11.2.7	Trebuie să fie posibilă extinderea SMAE, într-o manieră controlată, pentru a corespunde creșterii organizației până la cel puțin <xx sute/mii> utilizatori, cu păstrarea continuității de funcționare.	N

Ref	Cerințe exemplu	Testabil
	Intenția acestei cerințe este ca mărirea să poată fi posibilă doar cu ajutorul actualizărilor obișnuite, care nu generează întreruperi majore ale funcționalității.	
11.2.8	SMAE trebuie să susțină nivelul de performanță de mai sus, inclusiv întreținerea regulată a: ▪ rolurilor, utilizatorilor și a grupurilor de utilizatori; ▪ categoriilor de securitate; ▪ profilelor de acces; ▪ schemelor de clasificare; ▪ bazelor de date; ▪ programării de păstrare și dispoziție; ▪ blocărilor/suspendărilor de dispoziție; în perspectiva nivelurilor anticipate ale schimbărilor organizaționale, fără a genera pauze operaționale în sistem sau supraaglomerări ale contului de administrator (vezi de asemenea capitolul 9). *În cazurile în care cerințele de performanță sunt stricte, poate fi necesar să se cuantifice nivelurile anticipate ale modificărilor organizaționale.*	N
11.2.9	SMAE trebuie să fie scalabil și trebuie să poată fi folosit în organizații mai mari sau mai mici, cu un număr variabil de structuri organizaționale de diferite mărimi și plasate în diferite locuri din punct de vedere geografic.	N

11.3 Disponibilitatea sistemului

În multe organizații, introducerea unui SAME sau a unui SMDE va spori dependența utilizatorilor de rețeaua IT, până la nivelul la care ei nu își vor putea continua activitatea dacă SAME sau SMDE devin indisponibile.

În consecință, utilizatorii acestei specificații care deschid o licitație pentru un sistem ar trebui să facă toate eforturile pentru a identifica cerințele utilizatorilor pentru disponibilitate, și să specifice acest lucru în caietul de sarcini. Cerințe exemplu pentru disponibilitate sunt furnizate mai jos.

Ref	Cerință exemplu	Testabil
11.3.1	SMAE trebuie să fie disponibil pentru utilizatori: de la <xx:00> la <xx:00> <în fiecare zi /în toate zilele săptămânii/ /xx zile pe an>.	N

Ref	Cerință exemplu	Testabil
11.3.2	Nefuncționările planificate pentru SMAE nu trebuie să depășească <XX> ore pe <durata a trei luni consecutive>. *Definiția „nefuncționării" poate varia în funcție de infrastructură și arhitectura sistemului. De pildă, în anumite medii, o pană cauzată de hardware-ul server va fi considerată ca o pană a SMAE; în alte medii, o astfel de cădere va fi considerată un alt fel de pană, ce nu poate fi atribuită SMAE.* *Trebuie să se convină asupra unei definiții potrivite; ca punct de pornire, se propune următoare definiție: „SMAE se consideră a fi în pană dacă mai mult de <xx%> dintre utilizatori nu pot desfășura nici o funcție normală a SMAE și dacă pana se poate atribui oricărei componente a unui SMAE, alta decât cea a stației de lucru a utilizatorului.*	N
11.3.3	Nefuncționările neplanificate pentru un SMAE nu trebuie să depășească <XX ore/minute> pe <durata a trei luni consecutive>. *Într-o achiziție poate fi potrivit să se solicite o dovadă cantitativă despre timpul mediu de rezolvare a problemelor, ca sprijin pentru această cerință.*	N
11.3.4	Numărul de incidente de nefuncționare neplanificată pentru un SMAE nu trebuie să depășească <xx> pe <trei luni consecutive>. *Într-o achiziție poate fi potrivit să se solicite o dovadă cantitativă despre timpul mediu între pene, ca sprijin pentru această cerință.*	N
11.3.5	În cazul unei pene a oricărui alt software sau hardware, trebuie să fie posibil ca SMAE să revină la un stadiu cunoscut (nu mai vechi de <copia de siguranță a zilei anterioare>) cu nu mai mult de <xx> ore disponibile de activitate hardware.	N

11.4 Standarde tehnice

SMAE ar trebui să fie conform cu standardele de drept și de fapt aplicabile. Când este posibil, este de dorit ca SMAE să poată folosi interfețe deschise și nu brevetate.

Utilizatorii acestei specificații pot avea nevoie să specifice cerințele pentru standarde care se referă la:

- mediul hardware (pentru mediul de server și de stații de lucru);
- mediul sistemului de operare (pentru mediul de server și de stații de lucru);
- arhitectura de software a stației de lucru (client);
- interfața pentru utilizator;
- interfață și baza de date relațională;

- protocolul de rețea și sistemul de operare al rețelei;
- standard de schimb;
- interfața programelor aplicație și kiturile de dezvoltare.

La folosirea acestei specificații pentru achiziții, va fi necesar să se adauge noi detalii ale mediului tehnic, inclusiv toate interfețele SMAE (de pildă, sistemele moștenite, sistemele office) și orice planuri pentru schimbare.

În plus, utilizatorii acestei specificații vor trebui să ia în considerare cerințele lor individuale pentru standarde.

Vezi anexa 7 pentru o listă finală a standardelor utilizate în această specificație.

Ref	Cerințe model	Testabil
11.4.1	Dacă un tezaur monolingv este implementat odată cu SMAE, acesta ar trebui să fie conform cu standardul ISO 2788: *Linii directoare pentru stabilirea și dezvoltarea unui tezaur monolingv*.	D
11.4.2	Dacă un tezaur multilingv este implementat cu SMAE, acesta ar trebui să fie conform cu standardul ISO 5964: *Linii directoare pentru stabilirea și dezvoltarea unui tezaur multilingv*.	D
11.4.3	SMAE trebuie să accepte stocarea actelor folosind formatele de fișiere și codarea care sunt fie standarde de drept, fie sunt complet documentate. *Utilizatorii pot dori să precizeze formatul fișierelor și cerințele de codare pentru organizația lor.*	P
11.4.4	SMAE ar trebui să stocheze toate datele într-un format conform cu ISO 8601: *Elemente de date și formate de schimb — schimbul de informație — Reprezentarea datei și orei*.	D
11.4.5	SMAE ar trebui să stocheze toate numele limbilor într-un format conform cu ISO 639: *Coduri pentru reprezentarea numelor limbilor*.	D
11.4.6	Dacă SMAE trebuie să administreze acte în mai multe limbi sau folosind caractere diferite de cele ale limbii engleze, el ar trebui să fie capabil să gestioneze codarea tip ISO 10646 (Unicode).	D

11.5 Cerințe legislative și de reglementare

SMAE trebuie să se conformeze cerințelor legislative și de reglementare, care, de obicei, variază de la o regiune la alta și între industrii.

MoReq2 nu tratează problema păstrării actelor fizice. O astfel de nevoie poate, sau nu, să existe conform mediului legislativ și de reglementare; acolo unde o astfel de nevoie există, trebuie luate

măsuri pentru a prezerva integritatea și utilizabilitatea actelor fizice și electronice, ca un întreg. Aceste aspecte ar trebui să fie tratate de politicile corespunzătoare ale organizației.

Următoarele cerințe vor necesita adaptare locală, în „Capitolul Zero”.

În plus, utilizatorii MoReq2 vor trebui să ia în considerare cerințele care sunt specifice industriei înc are își desfășoară activitatea, sectorul economic etc.

Ref	Cerință	Testabil
11.5.1	SMAE trebuie să se conformeze la standardele aplicabile pe plan local, pentru admisibilitatea juridică și valoarea probatorie a actelor electronice.	N
11.5.2	SMAE trebuie să se conformeze cu la legislația aplicabilă pe plan local în domeniul *records management*-ului (arhivelor la creatori)	N
11.5.3	SMAE nu trebuie să includă nici o caracteristică ce este incompatibilă cu legislația aplicabilă pe plan local în domeniul protecției datelor personale, libertății de informare sau alte asemenea.	N
11.5.4	SMAE trebuie să se conformeze cu orice cerință de reglementare aplicabilă pe plan local, de nivel european, național sau local, cu coduri de practică specifice industriilor, funcțiilor de activitatea sau sectoare economice.	N

11.6 Externalizare și managementul datelor de către terți

Multe organizații folosesc furnizori externi de servicii pentru a stoca și administra acte. În anumite cazuri, acestea sunt acte ce nu mai sunt active (sau sunt mai rar folosite), dar care trebuie păstrate pentru o durată stabilită prin prevederi legale sau guvernamentale, reglementări ale industriei sau pentru termen lung.

Alte organizații folosesc furnizori de servicii de aplicații (Application Service Providers, ASP) pentru a administra actele active ca și pe cele care au fost arhivate. Organizațiile transmit documentele sau actele — facturi, corespondență cu clienții, documentele pentru cereri de ipotecă etc. — pentru a fi indexate și stocate prin ASP. Documentele sunt apoi disponibile pentru regăsire de către personalul organizației prin Internet sau printr-o rețea de mare suprafață.

Managementul actelor electronice de către terți cere ca în contractul cu furnizorul de servicii să fie clar definite proceduri și evidențe cu scopul de a satisface cerințele de reglementare, de a adera la bunele practici privind admisibilitatea legală a actelor electronice și să satisfacă cerințele activității clientului pentru acces și disponibilitate.

Contractul va trebui să includă prevederi precum că:

- administrarea furnizorului de servicii trebuie să fie în mod standard cel puțin la fel de bună ca și cea a administrării interne a clientului asupra propriilor acte.
- clientul va putea să recupereze actele de la furnizorul de servicii în viitor, și să fie capabilă încă să continue managementul actelor la standardele organizației și să satisfacă cerințele de admisibilitate legale.

Această sub-secțiune se inspiră masiv din ISO 15801 (vezi anexa 7).

Ref	Cerință	Testabil
11.6.1	Un contract sau o înțelegere la nivel de serviciu (Service Level Agreement, SLA) trebuie să fie convenită cu furnizorul de servicii, detaliind serviciile care vor fi folosite.	N
11.6.2	O SLA este o înțelegere negociată oficial, între clienți și furnizorul de servicii. El consemnează pozițiile asumate în ceea ce privește serviciile, prioritățile, responsabilitățile etc.	
11.6.3	Detaliile procedurilor pentru transferul actelor de la client către furnizorul de servicii și de la furnizorul de servicii către client trebuie să fie documentate.	N
11.6.4	*Se pot folosi legături de comunicație între diverse locuri pentru transferul dosarelor și actele în mod automat, cu o frecvență zilnică sau periodică. Clientul trebuie să fie asigurat că legătura între cele locuri este sigură și că protocoalele sunt implementate pentru a verifica toate actele primite și să producă rapoarte care să listeze orice inadvertență.*	
11.6.5	Furnizorul de servicii trebuie să poată furniza clientului copii ale evidenței de auditare ale proceselor, pentru logare și stocarea actelor/dosarelor.	N
11.6.6	Furnizorul de servicii trebuie să demonstreze că dosarele/actele și metadatele stocate pot fi transferate cu ușurință înapoi către SMAE clientului, fără nici o pierdere a structurii, metadatelor sau conținutului actelor.	N
11.6.7	Furnizorul de servicii trebuie să aibă implementate proceduri pentru a permite clientului să transfere dosare și acte individuale.	N
11.6.8	Furnizorul de servicii trebuie să poată furniza un acces prompt al clientului la actele administrate. Furnizorul de servicii trebuie fie să livreze clientului o prezentare a actului sau actul original, într-un timp și la un preț negociat.	N
11.6.9	Furnizorul de servicii ar trebui să-i poată oferi clientului abilitatea de a solicita, vizualiza și tipări acte și/sau dosare din birourile clientului.	N
11.6.10	*Aceasta poate fi realizată, de pildă, prin intermediul unei conexiuni de rețea.*	
11.6.11	Furnizorul de servicii ar trebui să poată furniza clientului posibilitatea de a solicita on-line descărcarea sau transmiterea actelor și/sau dosarelor între SMAE clientului și spațiul de stocare al furnizorului de servicii.	N

Ref	Cerință	Testabil
11.6.12	Clientul ar trebui să poată solicita rapoarte asupra actelor păstrate de furnizorul de servicii și detalii asupra programării de păstrare și dispoziție etc. Această facilitate ar trebui să fie oferită online din birourile clientului.	N
11.6.13	Serviciile specificate în cerințele 11.6.7, 11.6.8, 11.6.9 ar trebui: ▪ să aibă prevăzute în contract timpi de răspuns și reacție; ▪ să opereze într-un mediu securizat.	N
11.6.14	Clientul ar trebui să verifice dacă locul propus pentru activitate este acceptabil și dacă amplasamentul îndeplinește criteriile corespunzătoare pentru nevoile clientului.	N
11.6.15	Clientul ar trebui să verifice dacă procedurile propuse și procesele de administrare a stocării/depozitării nu implică un risc mai mare pentru acte decât propriile proceduri ale clientului.	N
11.6.16	*Furnizorul de servicii va trebui să demonstreze că toate actele clientului au copii de rezervă și că în cazul unei pene a sistemului acestea pot fi recuperate în perioada de timp prevăzută în contract.*	
11.6.17	Clientul ar trebui să verifice dacă furnizorul de servicii va furniza personal operațional corespunzător acolo unde securitatea actelor este importantă.	N
11.6.18	*Este un avantaj dacă toți angajații furnizorului de servicii semnează o înțelegere de confidențialitate ca parte a condițiilor lor de angajare.*	
11.6.19	Fiecare transport de acte între client și furnizorul de servicii ar trebui să fie însoțit de un document de evidență, care să precizeze identitatea și numărul actelor și dosarelor.	N
11.6.20	Terții care furnizează servicii de transport ar trebui să fie organizații care satisfac criteriile de calitate și încredere ale clientului.	N

11.7 Prezervarea pe termen lung și învechirea tehnologică

Preliminarii

Actele electronice păstrate pentru termen lung întâmpină riscuri tehnologice din trei direcţii:

- degradarea suportului;
- îmbătrânirea (*obsolescence*) hardware;
- îmbătrânirea formatului.

Aceste aspect sunt discutate pe scurt mai jos. Consideraţii mai detaliate se pot găsi in ISO 18492şi într-un mare număr de publicaţii de îndrumare, publicate de instituţii ale memoriei culturale şi altele.

Degradarea suportului

Riscul degradării suportului apare deoarece toate suporturile de stocare digitale au o durată de viată limitată. Durata de viaţă variază între suporturi şi de asemenea în funcţie de condiţiile de mediu.

Următoarele precauţii trebuie luate pentru a preveni pierderea informaţiilor din cauza degradării suportului:

- asigurarea că toate suporturile sunt stocate, folosite şi manipulate în condiţii corespunzătoare de mediu;
- înlocuirea periodic a suportului (prin copierea informaţiilor pe un suport nou), înainte de sfârşitul estimat al duratei de viaţă;
- păstrarea câtorva copii ale fiecărui act şi compararea sistematică, de o manieră periodic, a copiilor. Această abordare este în mod obişnuit folosită în arhivele de date specializate pe termen lung; presupune sisteme automate, o descriere mai amplă a acestora fiind în afara domeniului acestei specificaţii.

Îmbătrânirea hardware

Dispozitivele periferice de stocare — benzi, discuri — au o durată de viaţă limitată. Cu cât sunt mai aproape sau cu cât depăşesc această durată de viaţă aşteptată, acestea solicită mai multă muncă de mentenanţă, devenind în acelaşi timp mai scump de întreţinut şi reparat; în cele din urmă, ele devin de nereparat, din raţiuni practice. Informaţiile stocate pe dispozitive îmbătrânite vor fi pierdute permanent atunci când dispozitivele intră în pană, dacă acestea nu au fost anterior copiate pe alt suport.

Îmbătrânirea formatului

Îmbătrânirea formatului este cea mai dificilă problem pentru orice perioadă mai lungă de câţiva ani.

Problema apare deoarece cele mai multe component de aplicaţii şi protocoale implicate în ,,lanţul" de prelucrare între suport şi informaţiile prezentate evoluează constant. Ele include standarde de codificare, formate de fişiere şi aplicaţii. Evoluţia lor este rapidă, şi adesea nu păstrează compatibilitatea — lucru adevărat mai ales pe perioade mi lungi de câţiva ani. În prezent, următoarele tehnici sunt recunoscute:

- migrarea (conversia informaţiei în noile formate care pot fi accesate de software şi hardware actual);
- emularea (mutarea informaţiei pe noi hardware, dar cu o componentă software suplimentară care emulează (simulează condiţiile de pe) vechiul hardware, permiţând astfel executarea vechilor aplicaţii);

- prezervarea tehnologiei (întreținerea continuă a hardware-ului original; nu este practică pe termen lung);
- încapsularea datelor şi a software (o abordare teoretică ce implică împachetarea laolaltă a actelor, metadatelor, SMAE şi a altor software într-un software ,,ambalaj" standard;

Nu există, în momentul redactării, nici o metodă universală care va garanta accesul pe termen lung la actele electronice. Consensul este că:

- cea mai potrivită strategie este de a păstra informaţia doar în formate deschise, stabile, larg acceptate (adică, formate care sunt complet documentate în specificaţii disponibile publicului) care au o speranţă de viaţă îndelungată, cum ar fi XML şi PDF/A;
- migrarea şi/sau emularea par a fi cele mai sigure opţiuni; în practică, ambele vor necesita atenţie la prezervarea metadatelor — vezi mai jos.

Cerinţele din această secţiune sprijină aceste abordări. Mai multe surse de informaţie sunt furnizate în anexa 7.

Cerințe specifice

Ref	Cerinţă	Testabil
11.7.1	Suportul de stocare al SMAE trebuie să fie folosit şi stocat în medii care sunt compatibile cu durata de viaţă dorită/aşteptată şi care este în limitele de toleranţă precizate în specificaţia fabricantului suportului.	N
11.7.2	SMAE trebuie să accepte monitorizarea şi înlocuirea suportului de stocare pentru a preveni degradarea suportului. *Această cerință prevede ca SMAE, sau sub-sistemul de stocare pe care îl foloseşte, să raporteze asupra ratelor de eroare ale suportului şi să permită înlocuirea suportului care are defecte sau care este aproape de sfârşitul durate de viaţă sale, fără a afecte actele.*	D
11.7.3	SMAE ar trebui să includă caracteristici pentru compararea automată, periodică a copiilor informaţiilor şi să înlocuiască orice copie găsită cu defecte, pentru a asigura protecţia împotriva degradării suportului.	P
11.7.4	SMAE trebuie să permită migrarea masivă (redarea) actelor (împreună cu metadatele lor şi cu informaţiile din evidenţa de auditare) către noi suporturi şi/sau sisteme aliniate cu standarde relevante pentru formatul lor,	D
11.7.5	Furnizorul SMAE trebuie să aibă configurat un program pentru actualizarea sistemului, în scopul de a se asigura că informaţiile existente pot continua să fie accesate fără schimbări de conţinut.	N
11.7.6	Orice modificări de sistem care au fost făcute unui SMAE pentru cerinţele organizaţiei trebuie să rămână configurate după actualizarea unui sistem.	N

Ref	Cerinţă	Testabil
11.7.7	SMAE ar trebui să poată raporta despre formatul fişierelor şi versiunile componentelor. *De pildă, SMAE ar trebui să poată furniza liste de componente având un anume format de fişier. Această facilitate ar putea fi folosită împreună cu un* software intelligence *sau cu monitorizarea prezervării, funcţie care urmăreşte identificarea formatelor de fişiere care sunt supuse riscului de îmbătrânire.*	D
11.7.8	SMAE ar trebui să poată reda (vezi glosarul) acte din formatul(tele) lor original(e) în orice format(e) de fişier specificat pentru păstrarea pe termen lung la momentul capturării, şi la orice moment ulterior sau la exportare. *Este acceptabil ca procesul de redare să fie desfăşurat printr-un program exterior SMAE, atât timp cât contextul şi legăturile sunt păstrate în orice moment.*	P
11.7.9	Ori de câte ori este posibil, fără a afecta integritatea actelor, SMAE ar trebui să poată reda componentele din formatul lor original în orice format de fişier specificat pentru păstrare pe termen lung la momentul capturării, la un moment ulterior sau la exportare. *Se acceptă ca procesul de redare să fie desfăşurat de un program SMAE atât timp cât contextul şi legăturile sunt păstrate în orice moment.* *Acolo unde componentele sunt redate, este esenţial ca integritatea actelor pe care le formează să fie menţinută. Fezabilitatea acestei abordări va depinde în general atât de capacitatea procesului de redare cât şi de aplicaţia software sau programul de vizualizare folosit pentru a prezenta actele. De pildă, dacă actele sunt pagini web care include (să spunem) fişiere imagini GIF, ar fi acceptabil să fie redate imaginile GIF separate doar dacă următoarele elemente sunt adevărate:* ▪ *componentele GIF sunt redate într-un format de fişier care poate fi prezentat de aplicaţia folosită pentru a accesa paginile web; în acest exemplu, este probabil ca formatul JPEG să fie potrivit;* ▪ *referirile la imaginile GIF din pagina web este modificată ca parte a procesului de migrare, astfel încât ele să se refere în loc la noile imagini jpeg;* ▪ *componentele originale (paginile web nemodificate şi componentele GIF ne-redate) sunt reţinute împreună cu noile componente.*	P

Ref	Cerinţă	Testabil
	SMAE trebuie să accepte cel puţin aceste acţiuni şi ar trebui, în cazul cel mai fericit, să le desfăşoare automat. *Acest exemplu este ales doar cu scop de exemplificare; el nu indică, în momentul scrierii, că ar exista vreun motiv pentru care imaginile în format GIF ar trebui să fie migrate.*	
11.7.10	Ori de câte ori acte sau component sunt redate, SMAE trebuie să permităadministratorului care desfăşoarăredarea să introducă un motiv.	D
11.7.11	Atunci când un act a fost redat într-un format de prezervare, SMAE trebuie să furnizeze posibilităţi corespunzătoare de a regăsi formatul original şi/sau redările, după caz. *Vezi de asemenea5.2.3.*	P
11.7.12	SMAE ar trebui să poată exporta actele şi metadatele lor sub forma unui Pachet de Informaţii pentru Diseminare, aşa cum este acesta definit în anexa 7 a standardului OAIS, ISO 14721.	D
11.7.13	SMAE ar trebui să păstreze cel puţin următoarele elemente de metadate pentru componentele sale redate: ▪ formatul original ar fişierului şi versiunea; ▪ data redării.	D
11.7.14	SMAE ar trebui să poată extrage metadate tehnice stocate într-o component din acea component, şi apoi să le stocheze ca metadate. *Aceste metadate ar fi în completarea metadatelor specificate în modelul de metadate MoReq2. De pildă, poate include detail tehnice ale unei imagini, cum ar fi metadatele formatului TIFF, v. 6 sau ordinea byte-ilor (endian mic sau endian mare), lungimea şi lăţimea imaginii.*	P
11.7.15	Dacă SMAE foloseşte vreo structură de codare, stocare sau bază de date brevetate, acestea trebuie să fie complet documentate, documentaţia fiind disponibilă rolurilor de administrator. *Aceasta cerinţă implică faptul că nu este suficient pentru furnizor să păstreze o copie a documentaţiei; la orizontul de timp preconizat, stabilitatea unui furnizor nu este sigură. Poate fi, prin urmare, de dorit ca o copie a acestei documentaţii să fie încredinţată organizaţiei client sau unei părţi neutre.*	D
11.7.16	SMAE ar trebui să poată administra o varietate de elemente de metadate de prezervare pentru actele şi părţile sale component.	P

Ref	Cerinţă	Testabil
	Vezi anexa 9.	
11.7.17	Codul sursă al SMAE ar trebui fie să fie deschis fie o copie a acestuia ar trebui să fie depuse la un terţ.	N

11.8 Procesele de activitate

Experienţa a arătat că succesul instalării unui SMAE depinde, printre alţi factori, de măsura în care sistemul este compatibil cu felul în care oamenii lucrează în situaţiile reale. Chiar dacă un SMAE conţine toate caracteristicile necesare pentru managementul actelor, managementul documentelor etc., o implementare va reuşi doar dacă utilizatorii îl vor găsi uşor de folosit. Dacă utilizatorii îl găsesc dificil de folosit, ei îl vor respinge, în ciuda capacităţilor sale.

Ca o recunoaştere a acestei situaţii, această secţiune descrie cerinţele destinate pentru a promova flexibilitatea şi uşurinţa de folosire. În consecinţă, majoritatea cerinţelor sunt recomandabile şi nu obligatorii. Cerinţele pot fi satisfăcute de o aplicaţie de flux de lucru (*workflow software*) care este integrat cu SMAE.

Unele dintre cerinţele de mai jos fac referire la capacitatea de a desfăşura o anumită funcţie ,,ca parte integrantă a unui proces". În toate cazurile, aceasta înseamnă că un utilizator care desfăşoară un procesa ar trebui:

- să aibă opţiunea de a desfăşura (sau nu) un proces;
- să poată iniţia cu uşurinţă funcţia, de preferat cu un singur clic, şi fără a avea nevoie să re-introducă informaţiile care au fost deja introduse;
- să poată alege, la finalul funcţiei, fie să anuleze procesul original sau să se întoarcă la acesta în acelaşi punct şi cu aceeaşi stare ca înainte de iniţierea funcţiei (fără a avea nevoie să re-introducă informaţiile care au fost deja introduse).

Această situaţie este ilustrată în figura 11.1

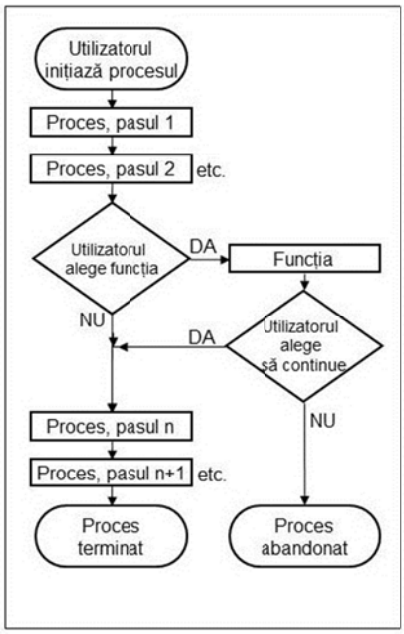


Figura 11.1

Toate cerințele care urmează trebuie să fie interpretate ca fiind dependente de drepturile de acces ale utilizatorului.

Ref	Cerinţă	Testabil
11.8.1	SMAE ar trebui să permit unui utilizator care are permisiunea de a modifica orice categorie de act, dosar sau clasă de a verifica respectiva categorie şi permisiunile aferente ca parte integrantă ale procesului de modificare.	D
11.8.2	Atunci când un utilizator rol de administrator este avertizat despre reducerea unei categorii de securitate a unui act (vezi 10.13.28), rolul de administrator ar trebui să poată examina actul şi/sau metadatele sale ca parte integrantă a procesului.	D
11.8.3	Ori de câte ori un nou dosar sau sub-dosar sunt create şi unde un container fizic există pentru ele, SMAE ar trebui să permit utilizatorului să imprime o etichetă corespunzătoare pentru containerul fizic, ca parte integrantă a procesului.	D

Ref	Cerinţă	Testabil
	Această cerință permite ca o etichetă care este produsă să conţină metadatele esenţiale, care apoi să fie anexate entităţii fizice. Aceasta ar putea include, dar nu este limitată, metadata precum: ▪ *Titlu;* ▪ *Identificatorul de sistem;* ▪ *Codul de clasificare;* ▪ *Data deschiderii;* ▪ *Categoria de securitate (dacă este folosită);* ▪ *Locul normal de* depozitare.	
11.8.4	Ori de câte ori un utilizator care şterge orice informaţie primeşte un avertisment despre legăturile existente (vezi secţiunea 9.3), utilizatorul ar trebui să poată examina legăturile şi informaţiile legate şi/sau metadatele lor, ca parte integrantă a procesului.	D
11.8.5	SMAE ar trebui să permit unui utilizator care reeditează un act, să realizeze următoarele, într-un singur proces integrat: ▪ să creeze o re-editare; ▪ să decidă unde ar trebui plasată în schema de clasificare acea re-editare şi să o declare ca act; ▪ să lege re-editarea de actul original; ▪ să lege actul original de re-editare.	D
11.8.6	Atunci când un utilizator declară un act, SMAE ar trebui să permită utilizatorului să verifice dacă un document a fost deja declarat ca act, ca parte integrantă a procesului. *Această cerință ar trebui să se aplice oricărui document, indiferent de formatul fișierului.*	D
11.8.7	SMAE ar trebui să avertizeze utilizatorul care capturează un document ca act dacă acel document a fost deja capturat, informând utilizatorul asupra locului în care este alocat (clasă, dosar etc.) şi să dea utilizatorului opţiunea de a continua procesul sau de a abandona capturarea.	D

Ref	Cerinţă	Testabil
11.8.8	Atunci când un utilizator capturează un act, SMAE ar trebui să permită să: ▪ parcurgă schema de clasificare (pentru a găsi dosarul, clasa etc. dorite); ▪ să vadă metadatele (permisiuni, cuvinte-cheie, descrieri etc.) ale oricăror clase şi dosare ▪ înainte de încheierea capturării, ca parte integrantă a procesului.	D
11.8.9	Ori de câte ori un utilizator vede orice clasă, dosar, act etc. pe ecran, ca rezultat al unei căutări, în timp ce parcurge schema de clasificare sau în orice alt context, utilizatorul ar trebui să poată desfăşura orice acţiune validă asupra lor direct, fără a avea nevoie să navigheze în altă parte a SMAE, incluzând cel puțin: ▪ să le deschisă; ▪ să determine structurile superioare din schema de clasificare; ▪ să vizualizeze metadatele lor sau evidenţa de auditare; ▪ să vizualizeze şi să urmărească legăturile lor; ▪ să le trimită prin e-mail; ▪ să le modifice categoriile de securitate; ▪ să vizualizeze utilizatorii şi rolurile care au acces permis la acestea; ▪ să le imprime (sau să le prezinte); ▪ să le re-editeze; ▪ să le repoziționeze sau să le şteargă.	D
11.8.10	SMAE ar trebui să permită unui utilizator autorizat să modifice categoria de securitate a oricărui act, dosar sau clasă, inclusiv actualizarea tuturor valorilor elementelor de metadate afectate, într-un singur proces.	D
11.8.11	Dacă un tezaur conform cu ISO 2788 sau ISO 5964 este integrat cu SMAE, SMAE ar trebui să permită unui utilizator care introduce sau actualizează o valoare cuvânt-cheie (sau altă valoarea a unui element de metadate înrudit cu tezaurul) să folosească toate caracteristicile unui tezaur, cum ar fi termeni hiperonimi, hiponimi şi asociați şi sinonime, ca parte integrantă a procesului. *De remarcat că11.1.18 conţine o cerinţă înrudită pentru căutare.*	D

12. Cerințe pentru metadate

Acest capitol prezintă cerințele funcționale pentru administrarea metadatelor. „Modelul” de metadate MoReq2 este prezentat în anexa 9. Secțiunea 12.1 acoperă principiile metadatelor și secțiunea 12.2 listează cerințele generale pentru metadate.

Metadatele include, în contextul prezentei specificații, informații de indexare și alte date necesare pentru administrarea eficientă a actelor, cum ar fi informații privitoare la restricțiile de acces. O definiție oficială este dată în glosar. O explicare mai detaliată a rolului metadatelor în managementul actelor se găsește în ISO 23081 (vezi anexa 7).

12.1 Principii

Arie de aplicare

Este imposibil să fie definite aici toate cerințele de metadate pentru toate posibilele tipuri de implementări SMAE. Diferitele tipuri de organizații și aplicați au nevoi particulare și tradiții de o extrem de mare varietate. De pildă, unele organizații vor avea nevoie de indexare bazată pe numele de cont și datele operațiunilor, în timp ce altele au nevoie strict de o numerotare ierarhică; unele vor avea nevoie de volume, care se referă la anul financiar, în timp ce altele nu; unele vor avea nevoie de un control al accesului pentru rațiuni de securitate, altele pentru protecția drepturilor intelectuale și așa mai departe.

Acest capitol al MoReq2 sugerează așadar cerințele minime care sunt gândite ca un punct de plecare pentru adaptare și dezvoltare. Aceste cerințe minime sunt strâns legate de lista specifică de „elemente”de metadate pe care SMAE trebuie să le poată captura și procesa. Aceste elemente formează modelul de metadate MoReq2 din anexa 9.

12.2 Cerințe generale de metadate.

Ref	Cerință	Testabil
12.2.1	SMAE nu trebuie să prezinte nici o limitare practică a numărului de elemente de metadate permise pentru fiecare entitate (de pildă, clasă, dosar, sub-dosar, volum, act). *Sensul expresiei „limitare practică” variază în funcție de aplicație. De pildă, unele organizații cu o schemă de clasificare simplă, ar putea să nu aibă nevoie de atât de multe elemente de metadate ca alte organizații, cu o schemă de clasificare complexă.*	P

Ref	Cerință	Testabil
12.2.2	Acolo unde conținutul elementului de metadată poate fi legat de comportamentul funcțional al SMAE, atunci SMAE trebuie să folosească conținutul acelui element pentru a determina funcționalitatea. *De exemplu, acolo unde SMAE stochează metadata „data de deschidere a dosarului", el trebuie să populeze acea metadată automat, ori de câte ori dosarul este deschis, în loc de a cere utilizatorului să o completeze. De remarcat că aceasta este o cerință generală, care se aplică mai multor elemente de metadate. MoReq2 nu încearcă să identifice toate cazurile în care această cerință este aplicabilă.*	P
12.2.3	SMAE trebuie să permită diferitelor seturi de elemente de metadată să fie definite pentru diferitele genuri de acte în momentul configurării sistemului. *De exemplu:* ▪ *facturile necesită metadata: „numărul contului";* ▪ *corespondența necesită elemente de metadate „destinatari", cu mai multe valori* ▪ *actele care sunt imagini scanate vor necesita metadate referitoare la procesul de scanare și indexare.*	D
12.2.4	SMAE trebuie să permită unui rol de administrator să definească, în momentul configurării sistemului, dacă fiecare element de metadată este obligatoriu sau opțional.	D
12.2.5	SMAE trebuie să accepte cel puțin următoarele formate de elemente de metadate: ▪ alfabetic; ▪ alfanumeric; ▪ numeric; ▪ dată; ▪ logic (de ex. YES/NO, TRUE/FALSE).	D
12.2.6	SMAE ar trebui să accepte ca rolul de administrator să poată defini formate pentru elemente de metadate, care constau în combinații ale formatelor definite le 12.2.5 *De pildă, un caz poate avea o cotă în formatul nnnnn/aa-n*	D
12.2.7	SMAE trebuie să accepte formatele de date definite în ISO 8601 pentru toate datele.	D

Ref	Cerință	Testabil
12.2.8	În momentul configurării sistemului, SMAE ar trebui să permită definirea sursei de date pentru fiecare element de medatată. *Posibilele surse sunt descrise în cerințele* **Error! Reference source not found.**, 12.2.10,**Error! Reference source not found.**și 12.2.13.	D
12.2.9	SMAE trebuie să permită unui rol de administrator să precizeze care valoare a elementului de metadate trebuie să fie introdusă și gestionată manual și care trebuie selectată dintr-un vocabular controlat.	D
12.2.10	SMAE ar trebui să permită ca valorile elementelor de metadate să fie moștenite automat în modul implicit de la nivelul imediat superior în ierarhia unei scheme de clasificare. *De exemplu, pentru un volum, valoarea unor elemente de metadate trebuie să fie moștenite de la sub-dosarul mamă; și pentru un act, valoarea unor metadate poate fi moștenită de la volumul în care sunt stocate.*	D
12.2.11	SMAE ar trebui să permită ca valorile pentru metadate să fie obținute din liste ascunse sau din apelarea altor aplicații. *De pildă, SMAE ar putea furniza numele și codul poștal prin apelarea unei aplicați pentru adrese care apoi generează numele străzii care trebuie folosit ca metadată.*	D
12.2.12	Acolo unde elementul de metadată este populat cu date din tabele legate, dacă selectarea unei valori depășește alte valori în tabelele legate subsecvente, aceasta ar trebui să se reflecte în valorile prezentate utilizatorilor în respectivele tabele subsecvente.	D
12.2.13	SMAE ar trebui să poată obține valori de metadate: ▪ dintr-o aplicație care creează documente (6.3.12); ▪ dintr-un sistem de operare; ▪ dintr-un program de rețea; ▪ de la utilizator, la momentul capturii sau declarării; ▪ prin regulile definite în momentul configurării pentru generarea de metadate de către SMAE la momentul declarării.	D

Ref	Cerință	Testabil
12.2.14	SMAE trebuie să poată valida metadatele atunci când acesta sunt introduse de utilizatori și atunci când sunt importate. Validarea trebuie să folosească cel puțin următoarele mecanisme: ▪ formatul conținutului elementului; ▪ interval de valori; ▪ validare cu o listă de valori, care este gestionată de un rolde administrator. *Un exemplu de validare de format este atunci când conținutul este integral numeric sau este în format tip „dată" (conform cu 12.2.5). Un exemplu de format dintr-un interval este atunci când conținutul este cuprins între 1 ianuarie 1999 și 31 decembrie 2001. Un exemplu de validare cu o listă de valori este verificarea dacă o destinație pentru exportare este prezentă într-o listă.*	D
12.2.15	SMAE trebuie să poată valida metadatele folosind apelarea unei alte aplicații (de pildă, a unui sistem de gestiunea resurselor umane pentru a verifica dacă un număr de angajat a fost atribuit, sau un sistem bază de date pentru coduri poștale) sau folosind un tabel intern legat.	D
12.2.16	SMAE trebuie să permită ca un rol de administrator să configureze validarea (așa cum este specificat la 12.2.14, 12.2.14) ce trebuie aplicată la fiecare element de metadate. *Diferite elemente de metadate necesită validări diferite. Deci, de exemplu, datele vor apela validare pentru format și interval, în timp ce descrierile nu vor necesita nici o validare.*	D
12.2.17	Pentru valorile elementelor de metadate care sunt introduse manual, SMAE ar trebui să permită unui rol de administrator să configureze elementul astfel încât acesta să accepte unul din următoarele moduri de introducere de date: ▪ valori implicite persistente definite de utilizator; ▪ o valoare predefinită constantă; ▪ data zilei de azi (doar pentru elementele tip „dată"); ▪ element liber. ▪ pot fi de asemenea acceptate moduri suplimentare pentru introducerea datelor, nespecificate mai sus,.	D

Ref	Cerință	Testabil
	O valoare predefinită persistentă apare ca predefinită în câmpul de introducere a datelor pentru fiecare element în succesiune până când este modificat de utilizator. Odată modificată, noua valoare este menținută, adică devine persistentă. Aceasta trebuie să persiste cel puțin până la sfârșitul unei sesiuni și la modul ideal, între sesiuni. Aceasta se aplică tuturor entităților pentru care utilizatorii pot introduce valori de metadate.	
12.2.18	SMAE ar trebui să permită configurarea astfel încât orice valoare a unui element de metadată să poată fi folosit ca și câmp de căutare într-o căutare de text liber.	D
12.2.19	Acolo unde o valoare a unui element de metadată este stocat în format „dată", SMAE ar trebui să permită căutări care recunosc valoarea datei. *De pildă, SMAE ar trebui să accepte căutări într-un interval de date. Nu este suficient ca datele să fie stocate într-un câmp tip text.*	D
12.2.20	Acolo unde valoarea elementului de metadată este stocată în format numeric, SMAE ar trebui să permită căutări care recunosc valoarea numărului.	D
12.2.21	SMAE trebuie să permită rolurilor de administrator să restricționeze posibilitatea de a face modificări la valorile de metadate, după cum este definit în modelul de control al accesului (secțiunea 13.4).	D
12.2.22	SMAE trebuie să permită reconfigurarea modelului de metadate al SMAE de către un rol de administrator, și trebuie să o înregistreze ca atare în evidența de auditare. *De exemplu, poate fi necesar ca noi elemente de date să fie adăugate, cum ar fi „Identificator de departament" pentru unele genuri de documente ce însoțesc modificări organizaționale.*	P
12.2.23	SMAE trebuie să permită elementelor de metadate să fie configurate în momentul configurării sistemului astfel încât valorile generate din alte pachete de aplicații, de sistemul de operare sau de SMAE (de pildă, datele de transmitere a e-mail-urilor) să nu poată fi modificate de utilizatori, odată ce acesta au fost capturate.	D
12.2.24	SMAE trebuie să permită elementelor de metadate să fie configurate în momentul configurării sistemului, astfel încât valorile lor să nu poată fi modificate de utilizatori odată ce ele au fost capturate.	D

13 Model de referință

Acest capitol furnizează un model de referință pentru cerințele prezentate în cadrul MoReq2. Secțiunile acestui capitol sunt:

- Glosarul (secțiunea 13.1)
- Schema grafică a modelului entitate-relație (secțiunea 13.2)
- Prezentare narativă a modelului entitate-relație (secțiunea 13.3)
- Modelul controlului de acces (secțiunea 13.4)

13.1 Glosar

Acest glosar defineşte termenii cheie folosiți în MoReq2.

Câteva definiții semnificative sunt preluate, sau puțin adaptate, după glosarele prezentate în publicațiile de referință precizate în anexa 1; aceste surse sunt făcute cunoscute sub fiecare definiție.

Termenii definiți în prezentul glosar sunt redați cu *italice*[8].

rol de administrator (*administrative role*)

Un set de permisiuni funcționale alocate *utilizatorilor* care desfăşoară acțiuni de administrare.

> Notă: în MoReq2 termenul este folosit şi pentru a indica persoanele ce au asemenea permisiuni.

administrator (*administrator*)

Un rol având responsabilitatea operațiunilor de zi cu zi ale politicii de management al actelor organizației, în cadrul organizației.

> Notă: această definiție este o simplificare. Mai ales în marile organizații, sarcinile atribuite în această specificație administratorilor pot fi distribuite mai multor roluri, denumite „manager al actelor”, „funcționar de arhivă”, „arhivist” etc.

grupare (*aggregation*)

[8] Notă la ediția românească: termenii originali din limba engleză sunt scrişi cu italice, în paranteză.

(doar în contextul MoReq2) O clasă, dosar, sub-dosar sau volum.

evidența de auditare (*audit trail*)

Informații despre operațiuni şi alte activități care au afectat sau schimbat entitățile (de ex. elementele de metadate), păstrate cu suficiente detalii pentru a permite reconstituirea unei activități anterioare.

> Notă: o evidență de auditare constă în general din una sau mai multe liste sau dintr-o bază de date care poate fi vizualizată sub această formă. Listele pot fi generate de un sistem informatic (pentru operațiunile sistemului informatic) sau manual (în general, pentru activitățile manuale), dar cele dintâi formează obiectul prezentei specificații.

autenticitate (*authenticity*)

(doar în contextul managementului actelor) Calitatea de a fi neschimbat.

Sursa: adaptat şi prescurtat după definiția „autenticitatea actului" din Glosarul UBC-MAS (anexa 1).

> Notă: un act autentic este unul despre care se poate demonstra că:
>
> „a). este ceea ce se afirmă că este;
>
> b). a fost creat sau emis de persoana care se afirmă că l-a creat sau transmis, şi
>
> c). a fost creat sau emis la momentul afirmat".
>
> Sursă: ISO 15489.
>
> Notă: în contextul unui *act*, această calitate implică faptul că un act este ceea ce se afirmă că este aceasta nu se referă la încrederea în conținutul actului ca o declarație de fapt.

utilizator autorizat (*authorised user*)

Un *utilizator* care are permisiunea de a desfăşura acțiunea descrisă.

> Notă: detaliile depind de context. Diverşi utilizatori pot avea diferite permisiuni. MoReq2 nu face nici un fel de presupuneri despre ce fel de permisiuni au diferitele roluri şi diferiții utilizatori. Permisiunile care autorizează un utilizator să desfăşoare o acțiune sunt acordate de organizație, în conformitate cu politicile şi cu cerințele sale de activitate.

importare masivă (*bulk importing*)

Procesul de captură a unui set de acte electronice, de obicei dintr-o altă aplicație şi de obicei cu o parte din sau cu toate metadatele acestora.

a captura (*capture*, verb)

(1) Acțiunea de înregistrare sau de salvare a unei instanțe particulare a unui obiect digital.

Sursa: InterPARES 2 Project Terminology Database.

(2). Salvarea informației într-un sistem informatic.

Notă: în contextul MoReq2, „a captura *acte*" este folosit pentru a înțelege toate procesele implicate în aducerea unui act într-un SMAE şi anume înregistrarea, clasificarea, adăugarea de metadate şi înghețarea conținutului documentului-sursă. Termenul este utilizat cu sensul mai general de a introduce într-un SMAE şi de a stoca alte informații cum ar fi valorile metadatelor.

dosar de caz (*case file*)

Un dosar care se referă la una sau mai multe operațiuni desfăşurate total sau parțial de o manieră structurată sau parțial structurată, ca rezultat al unui proces sau a unei activități concrete.

Notă: nu există o definiție universal acceptată a acestor termeni, nici o distincție între dosarele de caz şi alte categorii de dosare adesea administrate de SMAE. Această definiție este, prin urmare, dezvoltată pentru — şi urmărește să faciliteze înțelegerea — MoReq2; aplicabilitatea sa în alte situații nu este garantată.

Notă: actele dintr-un dosar de caz pot fi structurate sau nestructurate. Principala caracteristică distinctivă a dosarelor de caz este că acestea rezultă din procese care sunt cel puțin parțial structurate şi repetitive. Exemple include dosare despre:

- cereri pentru permise
- chestionare despre un serviciu de rutină
- investigarea unui accident
- monitorizarea regulamentară

Notă: în mod obişnuit, alte caracteristici ale dosarelor de caz sunt că acestea, în mod frecvent:

- prezintă o structură predictibilă a conținutului lor
- sunt numeroase
- sunt structurate sau în parte structurate
- sunt folosite sau administrate în cadrul unor procese cunoscute şi pre-determinate
- trebuie să fie păstrate pentru anumite perioade de timp, ca rezultat al legislației sau reglementărilor
- pot fi deschise şi închise de practicieni, utilizatori finali sau sisteme de procesare a datelor fără a fi nevoie de aprobarea conducerii

lucrător de caz (*case worker*)

Un *utilizator* care lucrează cu *dosare de caz*.

clasă (*class*, substantiv)

(doar în MoReq2) Porțiune a ierarhiei reprezentată de o linie pornind din orice punct al ierarhiei unei *scheme de clasificare* către toate dosarele aflate sub el.

> Notă: aceasta poate corespunde, în terminologia clasică, unei „clase primare”, „grup” sau „serii” (sau sub-clasă, sub-grup, sub-serie etc.), la orice nivel al schemei de clasificare.
>
> Notă: în MoReq2, „clasa” este de asemenea folosită pentru a denumi totalitatea actelor alocate unei clase.

clasificare (*classification*)

În managementul actelor, identificarea sistematică şi ordonarea activităților şi/sau *actelor* în categorii în conformitate cu metode, convenții şi reguli procedurale structurate logic, reprezentate într-un sistem de clasificare.

Sursă: ISO 15489 (vezi anexa 7).

codul de clasificare (*classification code*)

Un identificator atribuit fiecărei *clase* într-o *schemă de clasificare*. În cadrul fiecărei clase, codurile de clasificare ale claselor-copii sunt unice.

schemă de clasificare (***classification scheme***)

(în MoReq2) O ordonare ierarhică de clase, dosare, sub-dosare, volume şi acte.

autorizație (*clearance*)

Vezi *autorizație de securitate*

a închide (*close*, verb)

Procesul de modificare a atributului unui *dosar*, *sub-dosar* sau *volum*, astfel încât acesta să nu mai poată accepta adăugarea altor *acte*.

închis (*closed*)

Desemnează un *dosar, sub-dosar* sau *volum* care nu mai este deschis, deci nu mai poate accepta adăugarea altor *acte*.

CMS

Sisteme de management al conținutului (Content Management System)

componentă (*component*)

Un flux distinct de biți care, singur sau împreună cu alte fluxuri de biți, alcătuiesc un *act* sau un *document*.

Notă: acest termen nu este în uz general.

Notă: expresia „flux distinct de biți” este folosit pentru a desemna ceea ce în mod obişnuit este numit „fişier” (*file*) în tehnologia informației. Cuvântul *file* a fost evitat aici pentru a preveni confuzia cu sensul din managementul actelor al termenului *file* (dosar). Cheia conceptului este că o „componentă” este o parte integrantă a conținutului unui act, în ciuda faptului că el poate fi manipulat şi administrat separat.

Notă: exemplele de componente includ:

- un document HTML şi imagini JPEG, care compun o pagină web;
- un document dintr-un procesor de texte şi o foaie de calcul, unde actul constă din document care conține o legătură încorporată (o hiper-legătură) spre foaia de calcul.

Notă: componentele trebuie să fie distincte, adică separate una de cealaltă. Dacă un document dintr-un procesor de texte conține încorporată o foaie de calcul (spre deosebire de încorporarea unei legături către foaia de calcul), atunci se consideră că foaia d calcul nu este o componentă; în acest caz, documentul din procesorul de texte este un act alcătuit dintr-o singură componentă.

Notă: un mesaj e-mail cu anexe poate fi o componentă, precum şi câteva componente sau câteva acte, în funcție de formatul în care sunt stocate.

- Dacă mesajul este stocat într-un format care include corpul mesajului şi toate anexele sale, atunci este doar o componentă.
- Dacă anexele sunt stocate separat şi legate intern de corpul mesajului, atunci fiecare anexă şi corpul mesajului este o componentă.
- Dacă anexele sunt stocate separat de corpul mesajului de e-mail, dar ele nu sunt legate intern, atunci fiecare anexă şi corpul mesajului sunt câte un act separat; buna practică sugerează că aceste acte ar trebui să fie manual legate unul de altul.

momentul configurării (*configuration time*)

Punctul din ciclul de viață al unui SMAE la care este instalat şi îi sunt stabiliți parametrii.

custode (*custodian*)

(al unui act sau grupări) Persoana sau structura dintr-o organizație care are (au) în posesie actul(ele).

distrugere (*destruction*)

Procesul de eliminare […] a actelor, de o manieră care să nu mai permită sub nici o formă reconstituirea lor.

Sursa: ISO 15489 (vezi anexa 7).

Notă: în funcție de configurarea sistemului, termenul poate fi sinonimă cu ştergerea sau altă operațiune similară ştergerii.

Notă: Termenul nu urmărește să implice suprascrierea datelor distruse sau alte măsuri de securitate. Asemenea măsuri adiționale de securitate pot fi implementate, dar nu sunt cerute de MoReq2.

digital (*digital*)

Descrie informații alcătuite mai degrabă din digiți distincți sau valori numerice decât din valori continue variabile.

Notă: termenul nu este folosit în MoReq2 pentru a descrie acte. Deşi „acte digitale” este o expresie mai precisă decât „acte electronice”, primul este mai rar folosit în practică. Vezi *electronic.*

suspendarea dispoziției (*disposal hold*)

O regulă care împiedică *distrugerea sau transferul actelor.*

dispoziție (*disposal*)

Serie de procese asociate cu implementarea deciziilor de păstrare a *actelor*, *distrugerii* sau *transferului* care sunt documentate programări de dispoziție şi păstrare sau în alte instrumente.

Sursă: ISO 15489 (vezi anexa 7).

document (*document*, substantiv)

Informația înregistrată sau obiect care pot fi tratate ca un întreg.

Sursă: ISO 15489 (vezi anexa 7).

Notă: un document poate exista pe hârtie, microformă, suport magnetic au alt suport electronic. Poate include orice combinație de text date, grafică, sunet, filme sau alte forme de informație. Un singur document poate consta din una sau mai multe *componente*.

Notă: documentele sunt diferite de *acte* în câteva aspecte importante. MoReq2 foloseşte termenul document pentru a defini informația care nu a fost capturată ca *act*, respectiv clasificat, înregistrat şi verificat la ieșire. Cuvântul „înregistrat” (*recorded*) din definiție nu implică caracteristicile unui act (*record*). Totuşi, de remarcat că anumite documente devin *acte*.

genul documentului (*document type*)

Descrie documente care împărtăşesc anumite caracteristici comune.

Notă: de exemplu, documentele care au o machetă comună, conținut, cerințe de păstrare şi dispoziție şi/sau *metadate.* Genurile documentelor pot include, de pildă:

- formulare de cerere;
- corespondență (incluzând scrisori şi faxuri şi memoranduri);
- curriculm vitae;
- mesaje e-mail;
- factură;
- raport medical;
- pagină web.

Notă: în acest exemplu, mesajele e-mail sunt tratate diferit de alt fel de corespondență, deoarece pot avea diferite cerințe de metadate; nu este însă cazul în fiecare organizație.

Notă: fiecare organizație trebuie să îşi definească genurile sale documentare, în conformitate cu nevoile de activitate; exemplele de mai sus sunt pur ilustrative.

SMDE (*EDMS*)

Sistem de management al documentelor electronice.

Aplicație bazată pe calculator care se ocupă de managementul documentelor de-a lungul ciclului lor de viață.

Sursă: IEC 82045-1 Managementul documentelor

Notă: funcționalitatea cerută pentru un SMDE nu este inclusă în această specificație. Totuşi, un SMDE este adesea folosit în strânsă integrare cu un SMAE. Vezi secțiunea 10.3 pentru mai multe detalii.

electronic (*electronic*)

Pentru scopul acestei specificații, cuvântul „electronic” este folosit cu acelaşi sens ca „digital”.

Notă: înregistrările analogice, deşi ele pot fi privite ca electronice, nu sunt considerate „electronice” în sensul acestei specificații, deoarece ele nu pot fi stocate într-un computer decât dacă ele sunt convertite în format digital. Rezultă deci, în terminologia acestei specificații, că actele analogice pot fi stocate doar ca *acte fizice*.

document electronic (*electronic document*)

Un *document* care este în formă electronică.

Notă: termenul de *document electronic* nu este limitat la documentele textuale generate în mod obişnuit de procesoarele de texte. El include de asemenea mesaje e-mail, foi de calcul tabelar, grafice şi imagini, documente HTML/XML, documente multimedia sau compuse şi alte genuri de documente tip *office*.

act electronic (*electronic record*)

Un *act* care este în formă *electronică*.

> Notă: Un SMAE diferă de SMDE în câteva aspecte esențiale. Vezi secțiunea 10.3 pentru mai multe detalii.

a exporta (*export*, verb)

Procesul de producere a unei copii după *actele* electronice, împreună cu *metadatele* lor, pentru un alt sistem.

dosar (*file*, substantiv)

O grupare organizată de *acte* grupate împreună deoarece se referă la acelaşi subiect, activitate sau tranzacție (operațiune).

Sursă: prescurtat şi adaptat după ISAD(G) (vezi anexa 7).

> Notă: acesta este sensul din managementul actelor al termenului *dosar* (file). El diferă de sensul IT (*file* = *fişier*), pentru care MoReq2 foloseşte termenul *componentă.*

format de fişier (*file format*)

Structura internă şi /sau codificarea unui *act* sau*componentă*, care îi permite să fie prezentat într-o formă accesibilă pentru om.

Notă: exemplele includ:

- HTML v.3.2 (format de fişier pentru pagini web);
- PDF/A v.1 (format arhivistic de fişier pentru documente portabile).
- TXT (format de fişier tip text simplu ASCII)
- XML v.1.0 (un format de fişier pentru limbaj de marcare extensibil care se bazează el însuşi pe text simplu ASCII)
- multe formate de fişiere proprietate ,produse de aplicații pentru PC, cum ar fi pachetele *office*.

format (*format*, substantiv)

vezi *file format*

grup (*grup*, substantiv)

un set de *utilizatori*

> Notă: un grup poate include utilizatori cu roluri identice sau diferite. Un grup este uneori folosit pentru a defini afilierea utilizatorilor la o structură organizațională, cum ar fi un departament (în care caz va include, în mod obişnuit, câteva roluri); este uneori folosit

pentru a defini caracterul de membru al unei echipe virtuale care traversează cadrul organizațional, cum ar fi toate Birourile de achiziții (în care caz ar putea consta doar din utilizatorii cu un rol specificat); sau poate fi utilizat în alte feluri.

import (*import*)

vezi importare în grup

cuvânt-cheie (*keyword*)

Metadată opțională folosită pentru a descrie clase, dosare, sub-dosare şi acte, dar nu sub-volume.

Notă: buna practică este de a alege cuvintele cheie din — sau validate conform — unui vocabular controlat sau să fi extrase automat de un SMAE, dar acest lucru nu este obligatoriu.

metadată (*metadata*)

(în contextul managementului actelor) Date descriind contextul, structura şi conținutul actelor şi managementul acestora de-a lungul timpului.

Sursa: ISO 15489 (vezi anexa 6).

Notă: unele modele sunt bazate pe o perspectivă conceptuală diferită a metadatelor. De pildă, ele pot trata informațiile din evidența de auditare ca fiind în întregime metadate. Aceste perspective alternative sunt corecte şi valoroase în contextul lor, dar nu sunt de ajutor în specificarea funcționalității sistemelor şi de aceea nu sunt luate aici în considerare.

urmă de metadată (*metadata stub*)

Subset de metadate pentru un element, care este reținut după ce s-a dispus de acel element, pentru a servi drept mărturie că de elementul care fusese păstrat a fost supus unei proceduri de dispoziție într-o manieră corespunzătoare.

dosar general (*non-case file*)

Orice dosar care nu este un *dosar de caz*.

a deschide (*open*, verb)

Procesul de creare a unui nou *dosar*, *sub-dosar* sau *volum* ca atare, care pot accepta adăugarea de acte.

deschis (*open*, adjectiv)

Termen care descrie un *dosar*, *sub-dosar* sau *volum* care nu au fost încă *închise* şi care astfel încă au permisiunea de a accepta adăugarea de *acte*.

responsabil (*owner*)

Persona sau rolul responsabil pentru crearea sau gruparea unui act.

> Notă: termenul este folosit cu acest sens în MoReq2; proprietarul legal al unui act este organizația care deține acel act.

Notă: vezi de asemenea *custode*.

dosar hârtie (*paper file*)

O categorie de dosar fizic.

Notă: exemplele de dosare hârtie includ, printre altele, plicuri, dosare-cutii şi bibliorafturi.

PDF (*PDF*)

Format de document portabil, un *format de fişier* destinate în primul rând reprezentării informațiilor bidimensionale.

Notă: la momentul redactării, acest format larg folosit este proprietatea firmei Adobe, dar o versiune recentă a formatului (v.1.7) este în analiză pentru un Standard Internațional (ISO/DIS 32 000). Includerea termenului PDF în acest glosar nu reprezintă nici o formă de sprijin. Extensii pentru reprezentarea informațiilor tridimensionale sunt în curs de dezvoltare.

PDF/A (*PDF/A*)

Un subset al *PDF* proiectat pentru folosire arhivistică, aşa cum este definit în setul de standarde ISO 19005.

dosar fizic (*physical record*)

Un dispozitiv pentru păstrarea *documentelor fizice* şi a *actelor fizice*.

Sursă: adaptat după PRO Functional Specification (vezi anexa 1)

act fizic (*physical record*)

Un *act* care este ținut într-un mediu exterior unui SMAE, astfel încât actul însuşi nu este individual sub managementul SMAE.

Notă: exemplele includ actele pe hârtie, actele pe microforme şi actele electronice ținute pe suporturi amovibile, atât timp cât actele nu sunt administrate individual de către SMAE.

prezentare (*presentation*)

Manifestarea unui *act electronic* prezentat de SMAE la care un *utilizator* poate face referință.

Notă: natura precisă a prezentării poate fi afectată de mediul software şi hardware. În mod obişnuit, diferite prezentări ale aceluiaşi *act* pot varia în detaliile dimensiunilor de font, de capete de linie şi paginație, rezoluție, adâncimea bit-ului, spațiu de culoare etc. În majoritatea cazurilor aceste diferențe sunt acceptabile. Cu toate acestea, în unele cazuri efectele lor potențiale trebuie să fie distinct luate în considerație; aceste aspecte depăşesc domeniul acestei specificații.

Notă: în versiunea precedentă a MoReq2termenul *redare* a fost folosit cu acest sens.

profil (*profile*)

Un set de permisiuni alocate unui *utilizator* sau unui *grup* sau *rol*.

act (*record*, substantiv)

Informație creată primită şi păstrată pentru mărturie şi informare de o organizație sau persoană, rezultată din îndeplinirea obligațiilor legale sau dintr-o tranzacție/operațiune a unei activități.

Sursă: ISO 15489 (vezi anexa 7).

> Notă: pot fi luate în considerare de asemenea şi definiții naționale specifice.
>
> Notă: un act poate încorpora unul sau mai multe *documente* (de pildă când un document are anexe) şi poate exista pe orice mediu şi în orice format. În consecință, el poate fi alcătuit din unul sau mai multe *componente*. Pe lângă conținutul documentului (documentelor), un act ar trebui să includă informații contextuale şi, dacă este cazul, informație structurală (de pildă, informații care descriu componentele unui act). O caracteristică esențială a unui act este că el nu poate fi modificat.
>
> Notă: Un SMAE poate administra atât *acte electronice*, cât şi *acte fizice*.

genul actului (*record type*)

Descrie un *act* alcătuit dintr-un document cu *genul documentului* echivalent.

reedita (*redact*)

Procesul de ascundere a informațiilor confidențiale dintr-un *act*.

> Notă: aceasta poate include aplicarea unor dreptunghiuri opace pentru a acoperi numele etc. (echivalentul electronic pentru cenzurarea documentelor scrise cu cerneală), precum şi metode mai sigure de a ascunde informația sau eliminarea paginilor dintr-o copie a actului.
>
> Notă: în toate cazurile, nu este afectat *actul electronic* original în integralitatea lui. Reeditarea este realizată pe o copie a actului electronic; această copie se numeşte *reeditare*.

reeditare (*redaction*, substantiv)

(a unui act) O copie a uni *act* căruia i s-au aplicat o serie de modificări pentru a elimina sau masca, dar nu pentru a adăuga sau modifică înțelesul conținutului existent.

Sursa: definiția „instanței” din PRO Functional Specification (vezi anexa 1).

> Notă: schimbările rezultate, în mod obişnuit, din restricții asupra dezvăluirii de informații. De pildă, un *act* poate fi făcut public doar după ce numele persoanelor sunt acoperite sau înlăturate din el; în acest caz, este creată o reeditare a actului, din care numele au fost făcute invizibile. Procesul de mascare este uneori numit *redactare*.
>
> Notă: în ediția anterioară a MoReq2termenul „extras” a fost folosit cu acest sens.

înregistrare (*registation*)

Acțiunea de a atribui un identificator unic unui *act*, la intrarea acestuia într-un sistem.

Sursă: ISO 15489 vezi anexa 7).

> Notă: în contextul MoReq2, înregistrarea este o parte a procesului de *captură*.

reda (*render*)

Procesul de producere a unei *redări*.

întâlnire (*rendezvous*)

Un punct în fluxul de activități unde două sau mai multe activități paralele în execuție converg într-o singură serie comună de control.

Sursă: Workflow Management Coalition Terminology & Glossary, issue 3.0.

redare (*rendition*)

O manifestare a unui *act* sau a unei *componente* prin sau folosind sau mai multe *formate de fişiere* care sunt diferite de *formatul de fişier* nativ.

> Notă: redările sunt în general produse pentru a prezerva *actele electronice*, adică de a reduce riscul pierderii posibilității de acces a conținutului lor peste timp. De exemplu, actele produse intr-un format de fişier patentat poate fi stocat ca o redare într-un format standard, cum ar fi PDF/A sau XML.
>
> Redarea unui act înseamnă redarea unora sau a tuturor *componentelor* sale. După redare, actul poate avea acelaşi număr de componente ca înainte sau un număr diferit. De pildă, un act constând din 30 de componente incluzând 10 obiecte tip imagine GIF poate fi redat în câteva moduri, cum ar fi:
>
> Redarea unui act intr-un format de fişier PDF/A: în acest caz, actul inițial are 30 de componente, şi redarea are una.
>
> Redarea componentelor GIF doar într-un format de fişier JPEG: în acest caz atât actul cât şi redarea lui are 30 de componente şi, în plus, unele obiecte din redare trebuie să fie

schimbate pentru a face o referință corectă către noile imagini redare JPEG în loc de imagini GIF.

Notă: redarea a fost folosită cu diverse sensuri în versiunea originală a MoReq2.

inventar (*repertory*)

O listă a titlurilor de *dosare* existente în cadrul fiecăruia dintre cele mai mici niveluri ale schemei de clasificare.

programare de păstrare și dispoziție (*retention and disposition schedule*)

Un instrument oficial care defineşte perioadele de păstrare/reținere şi acțiunile de dispoziție ulterioare autorizate pentru actele descrise în regulă.

Sursă: adaptat după Glosarul de administrare al actelor întocmit de Arhivele naționale ale Australiei.

Notă: în versiunea anterioară a MoReq2 termenul folosit a fost programare de păstrare.

rol (*role*)

Gruparea unor permisiuni funcționale acordate unui subset predefinit de utilizatori.

Sursă**:** PRO Functional Specification (vezi anexa 1).

categoria de securitate (*security category*)

Unul sau mai mulți termeni asociați cu un *act* sau o *grupare* care defineşte reguli ce reglementează accesul la acestea.

Notă: categoriile de securitate sunt în mod obişnuit atribuite la nivel organizațional sau național. Exemple ale categoriilor de securitate folosite în organizațiile guvernamentale în majoritatea țărilor europene sunt: „strict secret de importanță deosebită” (*Top Secret*), „strict secret” (*Secret*), „secret” (*Confidential*), „secret de serviciu” (*Restricted*), „nesecret” (*Unclassified*). Acestea sunt uneori suplimentate de alți termeni cum ar fi: „exclusiv pentru Vestul Europei” sau „Personal”.

Notă: acest termen nu este de uz general. El a fost adoptat în MoReq2 în locul termenului „clasificare”, care este adesea folosit de către comunitatea serviciilor de securitate, pentru a evita confuzia cu sensul cuvântului *clasificare* din managementul actelor.

autorizație de securitate (*security clearance*)

Unul sau mai mulți termeni asociați cu un *utilizator* care defineşte *nivelurile de securitate* (*secretizare*) la care îi este acordat acces unui *utilizator*.

urmă (*stub*)

Vezi urmă de metadate (*metadata stub*).

sub-dosar (*sub-file*)

Subdiviziune intelectuală a unui dosar.

> Notă: sub-dosarele sunt adesea utilizate în mediile de management al dosarelor de caz. În mod obişnuit, fiecare sub-dosar este denumit şi fiecare sub-dosar este folosit pentru a stoca o anumită categorie sau categorii de acte pentru o instanță a cazului, cum ar fi „facturi”, „evaluări” sau „corespondență”. Acestea pot fi, totuși, folosite de asemenea și în medii cu dosare generale.

transfera (*transfer*, verb)

Procesul de mutare a *dosarelor electronice* complete, însoțite de *metadatele* lor, în alt sistem.

Sursă: adaptat după PRO Functional Specification (vezi anexa 1).

> Notă: dosarele sunt adesea transferate împreună cu toate celelalte dosare dintr-o *clasă* a *schemei de clasificare*, atunci când scopul transferului este de a muta dosarele într-o arhive, pentru păstrare permanentă.
>
> Notă: vezi de asemenea *export.*

utilizator (*user*)

Orice persoană care utilizează un SMAE.

> Notă: acesta poate include (printre alții) administratorii, personalul de birou, membri ai publicului şi personal extern, cum ar fi auditorii.
>
> Notă: un utilizator poate avea *roluri*, şi de asemenea să fie membru al *grupurilor*.

grup de utilizatori (*user group*)

Vezi *grup*.

profil de utilizator (*user profile*)

Profilul unui *utilizator*.

rol de utilizator (*user role*)

Un set de permisiuni funcționale alocate *utilizatorilor* care permit desfăşurarea de acțiuni care administrează actele.

Un *utilizator* poate avea mai multe *roluri de utilizator*, dar numai un singur *profil de utilizator*.

> Notă: în MoReq2 acest termen este folosit şi pentru a denumi persoanele care au astfel de permisiuni.

versiune (*version*)

(a unui *document*) Starea unui document la un anumit punct din timpul dezvoltării sale.

Sursă: PRO Functional Specification (vezi anexa 1)

> Notă: o versiune este în mod obişnuit unul din proiectele unui *document* sau documentul final. În anumite cazuri, totuşi, documentele finale există în câtva versiuni, de ex. manualele tehnice. În alte cazuri, versiuni sunt traducerile. Spre deosebire de documente, actele nu pot exista în mai mult de o versiune; vezi, de asemenea, *reeditare*.

act vital (*vital record*)

Un act care este esențial pentru funcționarea şi/sau supraviețuirea unei organizații în timpul şi/sau după o situație de urgență.

volum (*volume*)

O subdiviziune a unui sub-dosar.

> Notă: subdiviziunile sunt create pentru a îmbunătăți capacitatea de a administra conținutul sub-dosarelor, prin crearea de unități care nu sunt prea mari pentru a fi administrate corespunzător. Subdiviziunile sunt mai degrabă mecanice (de pildă, bazate pe numărul de acte sau pe serii de numere sau intervale de timp) decât intelectuale.

13.2. Modelul entitate-relație

Această secțiune repetă o aparte din secțiunea 2.3., pentru uşurința de informare.

Ea conține un model entitate-relație, care poate fi folosit ca un ajutor în înțelegerea specificației. Secțiunea 13.3 conține o explicație narativă care descrie şi explică modelul.

Modelul entitate-relație este prezentat în figura 13.3. Un aspect important al acestui model este că el nu are nevoie să reprezinte structuri existente stocate într-un SMAE. El reprezintă o perspectivă teoretică a entităților asociate cu acte. Un SMAE foloseşte aceste relații pentru a genera un comportament echivalent cu cel al structurilor din diagramă. Vezi secțiunea 2. pentru mai multe explicații asupra acestui subiect.

Relațiile între dosare, volume, acte şi alte entități importante sunt descrise în următorul model entitate-relație. Aceasta este o reprezentare formală a structurilor selectate care pot fi folosite pentru a descrie comportamentul unui SMAE.

În diagramă, entitățile — dosare, acte etc. — sunt reprezentate prin dreptunghiuri. Liniile care le unesc reprezintă relațiile dintre entități. Fiecare relație este descrisă printr-un text la mijlocul liniei şi aceasta ar trebui să fie citită în sensul săgeții. Fiecare capăt de sfârşit al relației are un număr car reprezintă numărul de apariții (altfel spus, cardinalitatea); numerele sunt explicate în legendă. Deci, de pildă, figura 13.1 semnifică „un act este compus din una sau maimulte componente” (de observat direcția săgeții relației).

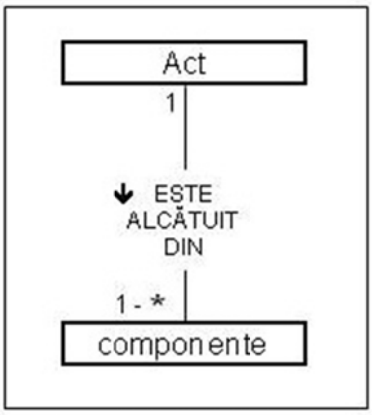


Figura 13.1

O linie curbă traversând două sau mai multe relații indică faptul că relațiile sunt reciproc excluse, pentru orice situație dată. Deci, de exemplu, linia curbă din figura 13.2 înseamnă „fiecare act este stocat fie într-un volum, fie într-un sub-dosar, dar nu în amândouă”.

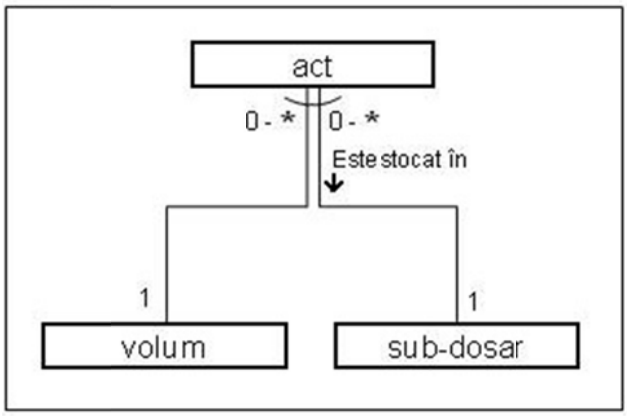


Figura 13.2

De observat că entitatea clasă se raportează la sine prin relația „este alcătuită din”. Această relație descrie, în termeni formali, relațiile dintre clasele dintr-o schemă de clasificare ierarhică, unde o clasă poate fi compusă din una sau mai multe alte clase. Dacă această relație (uneori denumită relație recursivă) este eliminată, modelul se aplică în egală măsură relațiilor non-ierarhice.

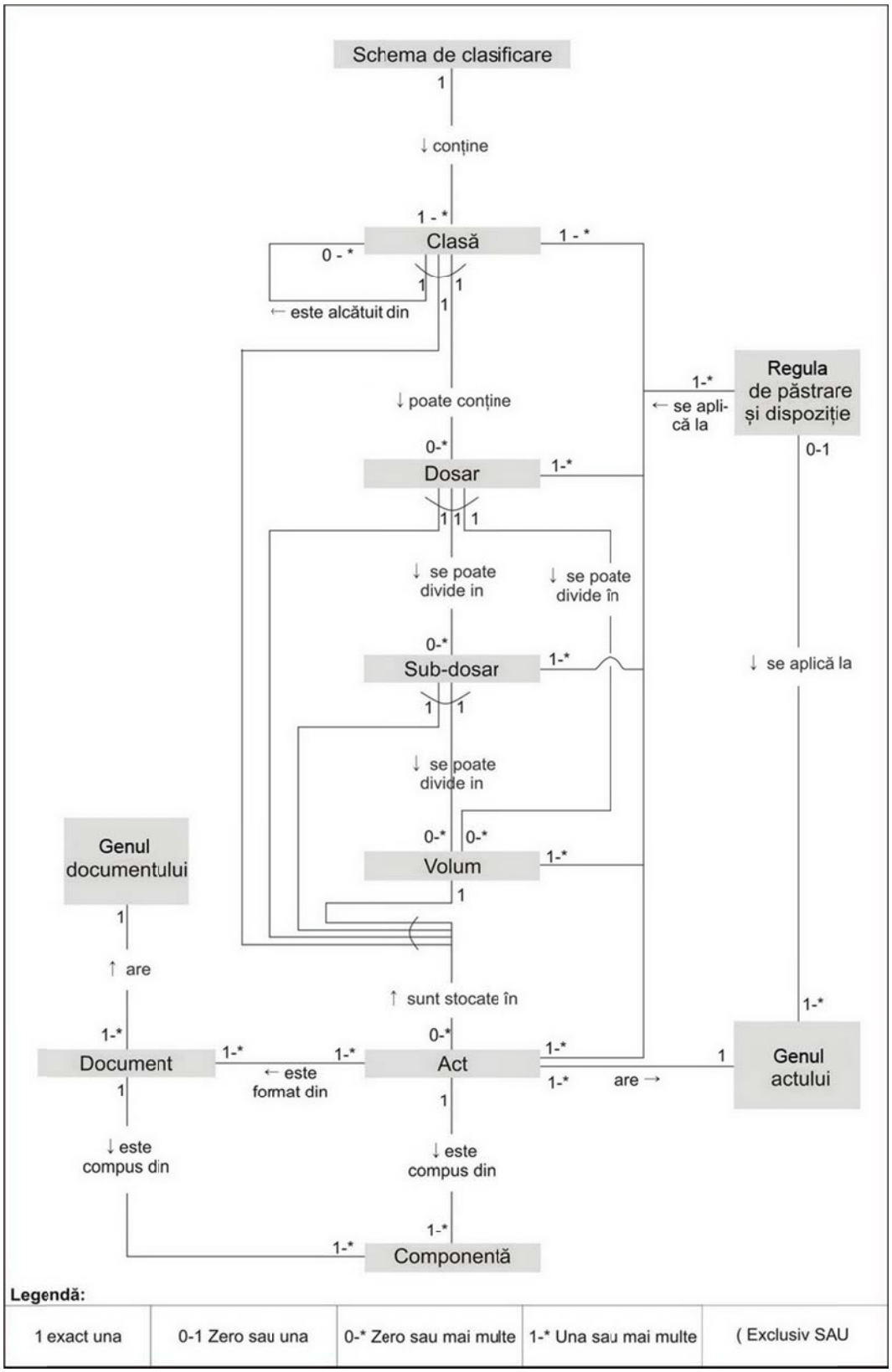

Schema de clasificare
1
↓ conține
1 - *
Clasă
1 - *
0 - *
1
1
1
← este alcătuit din
↓ poate conține
1-*
← se aplică la
Regula de păstrare și dispoziție
0-1
0-*
Dosar
1-*
1 1 1
↓ se poate divide in
↓ se poate divide în
0-*
Sub-dosar
1-*
1 1
↓ se poate divide in
↓ se aplică la
0-* 0-*
Volum
1-*
1
Genul documentului
1
↑ are
↑ sunt stocate în
1-*
0-*
1-*
Document
1-*
1-*
← este format din
Act
1-*
1-*
are →
1
Genul actului
1
1
↓ este compus din
↓ este compus din
1-*
1-*
Componentă
Legendă:
1 exact una
0-1 Zero sau una
0-* Zero sau mai multe
1-* Una sau mai multe
(Exclusiv SAU

Figura 13.3

13.3. Modelul entitate relație în formă narativă

Figura 13.3 prezintă un model simplificat; el nu încearcă să reprezinte toate posibilele entități sau relații. mai degrabă, el prezintă doar cele mai semnificative pentru această aplicație. De pildă, el nu prezintă utilizatori, roluri etc.

Restul acestei prezentări narative descrie entitățile din diagramă şi inter-relațiile lor.

Schema de clasificare

Pentru a pune în practică principiile managementului actelor, o organizație trebuie să aibă cel puțin o schemă de clasificare. Aceasta stabileşte structura de clasificare/a dosarelor (în mod obişnuit constând dintr-o ierarhie)pentru o parte definită a organizației. O schemă de clasificare conține câteva clase.

Clasă

Schemele de clasificare ierarhică pot fi văzute ca ierarhii alcătuite dintr-un număr de clase, la fel cum un copac este alcătuit din ramuri. Fiecare clasă este conectată la ierarhie la un anumit nivel; se poate extinde peste câteva niveluri; şi poate conține clase mai mici. Mai multe clase pot începe la acelaşi nivel; dar fiecare clasă începe doar la un singur nivel. Aşa cum este indicat prin relația tip „exclusiv SAU”, fiecare clasă poate:

- să fie alcătuită din clase; sau
- poate să conțină dosare; sau
- poate stoca acte

dar o combinație între acestea nu este posibilă.

Dosar

Dosarele apar în clase, la orice nivel al ierarhiei. Dosarele pot apărea doar în clasele care nu conțin alte clase. Aşa cum este indicat de relația „exclusiv SAU”, fiecare dosar poate:

- să fie divizat în sub-dosare; sau
- să fie divizat în volume; sau
- să stocheze acte;

dar combinația între acestea nu este permisă.

Sub-dosar

Fiecare dosar poate fi împărțit în sub-dosare (o opțiune de configurare stabileşte dacă sub-dosarele pot sau nu să existe). În practică, unele dosare nu sunt împărțite în sub-dosare. Acolo unde există doar un sub-dosar, conceptul de sub-dosar este uşor inteligibil pentru utilizatori, pentru toate scopurile practice. Sub-dosarele sunt adesea folosite în aplicațiile de management al cazurilor. Aşa cum este indicat de relația „exclusiv SAU”, fiecare sub-dosar poate:

- să fie divizat în volume; sau

- să stocheze acte;

dar o combinație a acestora nu este permisă.

Volum

Fiecare sub-dosar poate fi împărțit în volume (o opțiune de configurare stabileşte dacă volumele pot sau nu să existe), conform cu anumite reguli. În practică, cele mai multe sub-dosare nu pot fi divizate în volume. Acolo unde este doar un volum, conceptul de volum este uşor inteligibil pentru utilizatori, pentru toate scopurile practice. Regulile pot depinde de mărimea sau numărul actelor, sau poate depinde de tranzacții sau intervale de timp. Această practică îşi are originea în dosarele fizice, cu scopul de a le limita la dimensiuni şi greutăți administrabile. Practica, acolo unde e cazul, este continuată şi la dosarele electronice, pentru a le limita la o dimensiune administrabilă pentru revizuire, transfer etc.

Acolo unde un dosar constă din doar un sub-dosar, atunci volumele sale pot părea utilizatorilor mai degrabă volume ale dosarului decât un sub-dosar al său.

Termenii de dosar, sub-dosar şi volum sunt, în practică, uneori folosiți liber sau interschimbabil — din cauza cerinței de transparență de mai sus. De pildă, un utilizator va solicita în mod obişnuit „un dosar" şi nu (mai precis) „un volum". Acest lucru este cel mai adesea vizibil în situația unui dosar fizic, care conține un sub-dosar alcătuit dintr-un singur volum. În acest caz, deşi dosarul constă, la rigoare, dintr-un sub-dosar care este alcătuit dintr-un singur volum, sub-dosarul şi volumul nu sunt întotdeauna marcate ca atare (adesea, eticheta va fi aplicată doar atunci când va fi deschis al doilea sub-dosar sau volum).

Programarea de păstrare şi dispoziţie

O programare de păstrare şi dispoziţie specifică regulile pentru păstrarea şi dispoziția actelor. SMAE poate conține câteva programări de păstrare şi dispoziţie , din care una sau mai multe se pot aplica fiecărei clase, dosar, sub-dosar şi volum; ele pot de asemenea să fie aplicate actelor, şi o programare de păstrare şi dispoziţie poate fi aplicată fiecărui gen de act.

Act

În inima sistemului este cea mai importantă entitate, actul. Acesta este rațiunea de a fi pentru întreaga infrastructură de management al actelor, deoarece ele formează justificarea activităților organizației.

Actele sunt alcătuite din documente. Fiecare act poate cuprinde unul sau mai multe documente; şi fiecare document poate apare în mai multe acte.

Actele sunt în mod obişnuit stocate în volume. Totuşi, actele pot fi de asemenea stocate şi în clase (această este o excepție descrisă în altă parte). MoReq2 permite o opțiune de configurare care împiedică să fie utilizate volume şi/sau sub-dosare, în care cazuri actele vor fi stocate fie în sub-dosare sau în dosare. Fiecare act poate fi stocat doar într-un volum, sub-dosar, dosar sau clasă.

Genul actului

Actelor le sunt atribuite genuri. Aceste este folosit pentru a indica şi pentru a permite SMAE să administreze actele de o anumită manieră. Exemple de genuri de acte includ „factură” şi „pagină web”.

Componentă

Fiecare act şi document este alcătuit din cel puțin o componentă, unele sunt alcătuite din mai mult de una. De pildă, o simplă pagină web poate consta doar din o componentă — un fişier HTML — în timp ce pagini web mai complexe pot consta din zeci —un fişier HTML, fişiere GIF, fişiere JPEG şi aşa mai departe.

13.4 Modelul de control acces

Această secțiune conține un model simplu de roluri exemplu în cadrul unui SMAE.

Matricea recunoaşte două roluri principale, care sunt la rândul lor împărțite în roluri. Rolurile principale sunt rolurile de administrator şi de utilizator. Acestea sunt definite în termeni de acces la funcționalitățile SMAE.

Numărul de roluri prezentat în acest model este pur ilustrativ. El nu urmărește să indice că vreo organizație ar trebui să implementeze aceste roluri, nici ca vreo organizație ar trebui să implementeze acest număr de roluri. Fiecare organizație ar trebui să îşi definească rolurile de care are nevoie; şi aceste nevoi vor tinde să varieze de-a lungul timpului.

Aceste roluri de mai jos ilustrează un exemplu de drepturi de control al accesului pentru aspecte specifice ale funcționalității sistemului în conformitate cu responsabilitățile organizaționale.

Există patru exemple de roluri definite în această matrice exemplu:

Administrator central — acest rol are controlul configurării întregului SMAE şi al schemei sale de clasificare. Aceste roluri în mod obişnuit sunt folositoare în organizațiile dispersate geografic.

Administrator local — aceste este un rol cu drepturi de administrator asupra unui sub-set al SMAE sau al schemei sale de clasificare. Aceste roluri, în mod obişnuit sunt de folos în organizații dispersate geografic.

Revizor — acesta este un rol de specialist, care este în primul rând preocupat de aplicarea acțiunilor de dispoziție definite de programarea de păstrare şi dispoziţie .

Utilizator final — rolul de utilizator final este nivelul standard de acces într-un SMAE şi îi cuprinde pe cei care au nevoie să salveze acte în şi să acceseze acte dintr-un SMAE pentru activitatea lor obişnuită.

Rolurile de administrator sunt aici împărțite în rouă roluri doar cu titlu de exemplu; responsabilitățile pot fi împărțite în alte feluri. Pentru unele organizații mici, această împărțire ar putea fi inutil complicată, deoarece doar o persoană, cu un singur rol, poate conduce toată administrarea. Pentru organizațiile de amploare, ar putea fi o supra-simplificare, deoarece sunt necesare mai mult de două roluri (cum ar fi administratorul actelor, arhivar, arhivist şi administratorul de date sau administrator IT). MoReq2 nu încearcă să specifice câte roluri de administrator ar fi necesare în orice organizație reală.

Rolul administratorului local este furnizat aici ca un exemplu de acest tip. Acest rol poate avea diferite denumiri în diferite organizații. în anumite cazuri, acesta poate fi arhivarul local, sau un super-utilizator etc.

La orice eveniment, rolurile de administrator doar implementează, din perspective sistemului, deciziile luate de mai mulți reprezentanți ai managementului superior. Asemenea decizii sunt în mod obişnuit bazate pe cerințele de activitate ale organizației şi politică de administrare a actelor. Deciziile sunt impuse de asemenea de legi şi regulamente, cum ar fi legi ale liberului acces la informație, legi ale informațiilor secrete, legi arhivistice şi reglementări industriale; aceste aspecte sunt abordate în secțiunea 11.5.

Această matrice nu are intenția să afirme că rolurile de administrator trebuie să ia decizii de management, deşi în anumite situații poate să fie cazul.

Rolurile de administrator acționează în legătură cu managementul actelor înseşi; interesul lor este mai degrabă în managementul actelor ca entități decât in conținutul lor sau in contextul de activitate. Ele pot de asemenea să administreze componentele hardware, software şi de stocare ale SMAE, asigurându-se că sunt realizate copii de siguranță şi să administreze performanța SMAE.

Multe organizații au de asemenea nevoie de a integra managementul proceselor de afaceri cu managementul actelor. În aceste cazuri există o motivație pentru a aloca un set anume de permisiuni administrative pentru persoanele din managementul afacerii. Acestea pot include capacitatea de a urmări şi administra un anume grup de utilizatori sau o zonă din schema de clasificare.

Deşi MoReq2 se referă la un rol de utilizator, în majoritatea organizațiilor va exista un număr de diferite roluri de utilizatori şi SMAE nu ar trebui să limiteze numărul rolurilor care poate fi configurat.

Un exemplu al acestui fapt poate fi situația unui lucrător de caz (vezi secțiunea 10.5: *Activități de caz*). Un asemenea rol ar avea permisiuni specifice în cadrul unei anumite ramuri a schemei de clasificare.

Spre deosebire de rolurile de administrator, rolurile de utilizator au acces la facilități de care un lucrător de birou sau un cercetător are nevoie atunci când utilizează actele. Aceasta include adăugarea de documente, căutarea şi regăsirea de acte. Interesul lor este în primul rând orientat mai degrabă spre conținut, proprietăți sau contextul de afacere al actelor decât de managementul lor — cu alte cuvinte, ele sunt interesante de procesele de afaceri reflectate în acte.

În matrice, rolul unui utilizator final arată că drepturile de acces corespund în mod obişnuit celor pentru majoritatea utilizatorilor dintr-o organizație car îşi desfăşoară funcțiile lor specifice.

Un alt exemplu de rol de utilizator este dat: revizorul. Acesta prezintă un nivel de control al accesului, care poate fi alocat unui sub-set de utilizatori pentru scopul de revizuire a actelor.

Această matrice este cel mai bine vizualizată ca un punct de pornire şi ca o bază formală pentru atribuirea de drepturi. Utilizatorii acestei specificații vor avea nevoie să ia în considerare cerințe adiționale care sunt specifice mediului lor de lucru.

Cerințele formale care se referă la acest tabel sunt prezentate în secțiunea 4.1; ele confirmă că **cerința nu este ca un SMAE să încorporeze exemplul de matrice de acces prezentată aici, ci să fie capabil de a fi configurat la nivelul de detaliu al matricei de acces definite de organizația-client**, care poate conține un număr şi categorii de roluri şi funcțiuni nelimitate. Trebuie să fie posibil să

se configureze fiecare celulă a matricei ca DA sau NU, dar cu un tabel care are atâtea coloane câte are nevoie organizația.

Alte posibile roluri care pot fi implementate de organizație pot include, dar nu se limitează la:

- asistent
- auditor
- administrator pentru dreptul libertății de informare
- manager
- creator de acte
- administrator de acte
- supraveghetor

Această matrice este împărțită în secțiuni. Aceste secțiuni grupează, convențional, funcțiile asociate în mod normal cu clase şi doare, acte, managementul şi managementul actelor.

Funcție	Roluri			
	Roluri de utilizatori		Roluri de administrator	
	Utilizatori finali	Recenzori	Administrator locali	Administrator centrali
Adaugă noi clase	Nu	Nu	Da	Da
Creează noi dosare	Da	Nu	Da	Da
Schimbă metadate de dosar	Nu	Da	Da	Da
Întreține schema de clasificare şi dosarele	Nu	Nu	Da	Da
Şterge dosarele	Nu	Nu	Da	Da
Capturează actele	Da	Nu	Da	Da
Repoziționează un act într-un alt dosar	Da	Nu	Da	Da
Cercetează şi citeşte acte	Da	Da	Da	Da
Schimbă conținutul actelor	Nu	Nu	Nu	Nu
Schimbă metadatele actelor	Nu	Da	Da	Da
Şterge acte	Nu	Nu	Da	Da
Aplică şi înlătură suspendări de dispoziții	Nu	Da	Da	Da
Realizează programarea de păstrare şi dispoziție şi operațiunile de dispoziție.	Nu	Da	Da	Da
Exportă şi importă dosarele şi actele	Nu	Da	Da	Da

Funcție	Roluri			
	Roluri de utilizatori		Roluri de administrator	
	Utilizatori finali	Recenzori	Administrator locali	Administrator centrali
Vizualizează evidența de auditare	Nu	Da	Da	Da
Configurează şi administrează evidența de auditare	Nu	Nu	Nu	Da
Schimbă datele din evidența de auditare.	Nu	Nu	Nu	Nu
Mută datele din evidența de auditoare pe medii de stocare off-line	Nu	Nu	Da	Da
Desfăşoară toate operațiunile care se referă la utilizatori şi la privilegiile lor de acces.	Nu	Nu	Da	Da
Alocă permisiuni de acces administratorilor locali	Nu	Nu	Nu	Da
Alocă permisiuni de acces proprii şi altor utilizatori	Da	Da	Da	Da
Stabileşte şi administrează rolurile de management al cazurilor	Nu	Nu	Nu	Da
Întreține baza de date şi stocarea	Nu	Nu	Da	Da
Întreține alți parametrii de sistem	Nu	Nu	Nu	Da
Defineşte şi vizualizează alte rapoarte de sistem	Nu	Da	Da	Da

Anexa 1 —Referințe bibliografice

Această specificație a fost pregătită pe baza următoarelor specificații și publicații existente

Ref	Nume și deținător sau sursa	URL sau detaliile publicației
[1]	Dublin Core Metadata Element Set, Version 1.1: Reference Description	http://dublincore.org/documents/dces/
[2]	Functional Requirements for Electronic *records management* Systems (The National Archives of the UK)	http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/default.htm
[3]	Code of Practice for legal admissibility and evidential weight of information stored electronically (British Standards Institution)	Published by British Standards Institution (www.bsi-global.com) as BSIBIP 0008
[4]	The Preservation of the Integrity of Electronic Records (UBC-MAS Project)(University of British Columbia)	http://www.interpares.org
[5]	Standard 5015.2 “Design Criteria Standard For Electronic *records management* Software Applications” (US Department of Defense)	http://jitc.fhu.disa.mil/recmgt/
[6]	National Archives of Australia – Functional Specifications for Electronic *records management* Systems Software- Exposure Draft	The exposure draft is no longer available.A similar document is available from http://www.naa.gov.au/Images/ERMSspecifications_tcm2-1007.pdf

Ref	Nume și deținător sau sursa	URL sau detaliile publicației
[7]	Riksarkivet – The National Archives of Norway – NOARK-4 Norwegian recordkeeping system Version 4 – Part 1 Functional description and specification of requirements	http://www.arkivverket.no/arkivverket/lover/elarkiv/noark-4/english.html
[8]	Functional Requirements for the Sustainability of Electronic Records	http://www.nationalarchives.gov.uk/documents/functional_requirements.pdf
[9]	InterPARES 2 Project Terminology Database	http://www.interpares.org/ip2/ip2_terminology_db.cfm
[10]	DLM Forum Guidelines	http://dlmforum.typepad.com/gdlines.pdf

Anexa 2—Dezvoltarea acestei sepcificații

Privire generală

Specificația MoReq2a fost dezvoltată pentru Comisia Europeană de către o echipă de la Serco consulting (fosta Cornwell Management Consultants plc), cu sediul în Marea Britanie. MoReq2 se bazează pe un raport detaliat asupra obiectivelor, care a fost întocmit de către forumul DLM.

Echipa de proiect de la Serco a inclus consultanți specialiști, care au întocmit specificația, o mică echipă de management al proiectului și de administrare și un Colegiu de redacție, cuprinzând experți în *records management* din întreaga Europă și din America de Nord (vezi anexa 4). Una din versiunile finale a întregului document a fost revizuită de un revizor semi-independent.

Documentația pentru cadrul de testare a fost întocmită de o echipă de la Imbus AG.

Cerințele au fost supuse câtorva niveluri de revizuire.

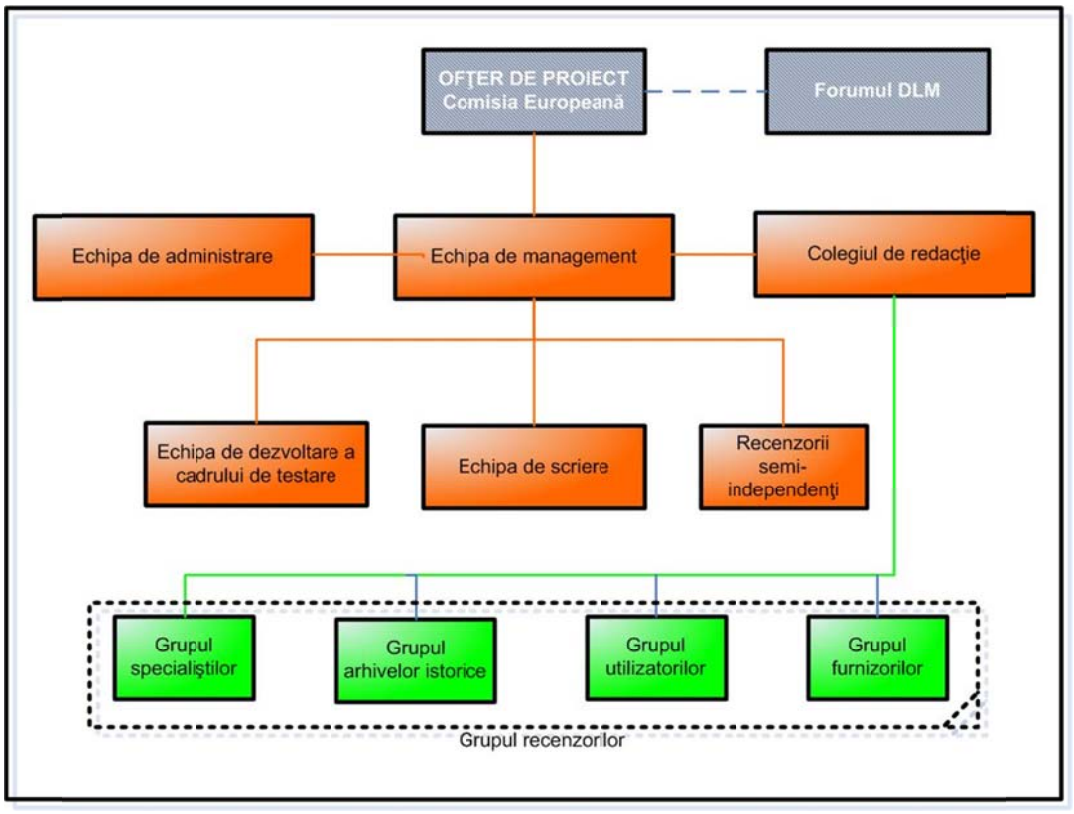
Mai întâi, membrii Echipei de scriere au procedat la revizuirea reciprocă a lucrărilor. Apoi, cerinţele proiect au fost transmise pentru procesul de revizuire unor grupuri reprezentând un spectru larg al părţilor interesate din comunitatea administrării actelor. Pentru o mai uşoară refernţiere, aceştia au fost grupaţi în:

- Grupul arhivelor istorice;
- Grupul specialiştilor;
- Grupul utilizatorilor;
- Grupul furnizorilor.

La intervale stabilite, proiectele au fost de asemenea revăzute de către Colegiul de redacţie MoReq2. Colegiul s-a întâlnit cu Echipa de Scriere în două ocazii, furnizând directive şi îndrumări de o deosebită valoare, iar membrii săi au procedat la a treia revizuire prin e-mail.

O versiune intermediată şi una ulterioară a MoReq2 a fost transmisă Comisiei Europene pentru aprobare. Proiectele au fost revizuite în numele Comisiei Europene de către un grup de revizuire al DLM Forum, costând din experţi renumiţi dintr-un eşantion reprezentativ al statelor membre UE.

Structura echipei de proiect este schiţată în figura A2.1; vezi şi anexa 4 pentru detalii asupra componenţei.



Figură A2.1

O întâlnire de debut a proiectului a fost ţinută la Londra, implicând echipa de scriere şi Colegiul de redacţie. La aceasta întâlnire, s-a convenit asupra protocoalelor de lucru şi a altor principii şi unele referinţe esenţiale au fost identificare. Aceasta a fost urmată de o cercetare de birou, şi de identificarea lucrărilor de referinţă relevante care sunt enumerate în anexa 1.

A fost desfăşurată o examinare atentă a lucrărilor de referință pentru a ne asigura că specificaţia revizuită cuprinde toate cerinţele relevante.

Versiunea originală MoReq2 a fost importată într-o aplicaţie (Teleologic DOORS), un pachet dedicat pentru managementul cerințelor şi modificărilor care a fost folosit de-a lungul procesului de scriere pentru a administra proiectele între membrii echipei şi pentru a urmări şi încorpora comentariile asupra proiectelor, venite din partea recenzorilor. Documentul a fost restructurat pentru a reflecta documentul cadru al MoReq2 astfel încât relațiile cu MoReq2 original să poată fi păstrate.

Odată cu definitivarea proiectului fiecărui capitol, acesta a fost publicat pe pagina web MoReq2şi toate grupurile au fost înştiinţate. Li s-a cerut să furnizeze contribuţiile lor într-un formular special proiectat pentru comentarii, care a permis integrarea comentariilor în aplicația DOORS, pentru a fi ulterior procesate de echipa de scriere.

Atunci când majoritatea capitolelor au fost făcute publice în acest fel, un proiect semi-complet al întregului document a fost alcătuit şi a fost transmis Colegiului de redacţie, în vederea identificării problemelor majore, înaintea celei de-a doua întâlniri Colegiului.

La această întâlnire, care de asemenea a fost ţinută la Londra, s-a ajuns la un consens între membrii asupra majorității problemelor care au fost identificare. Ca urmare, documentul a fost rescris în lumina celor convenite.

Noua formă a MoReq2 a fost transmisă Ofiţerului de Proiect al CE, şi membrilor Forumului DLM pentru revizuire. Evaluarea oficială a acestei versiuni interimare a fost transmisă firmei Serco şi discutată la întâlnirea de analiză a evoluţiei proiectului din Bruxelles.

Echipa de scriere a studiat toate comentariile primite, rezultate atât în urma revizuirii oficiale cât şi de la fiecare din celelalte grupuri, iar acestea au fost implementate sau respinse, după caz. Acest proces a fost intens şi repetat, deoarece multe dintre comentarii erau reciproc incompatibile sau nu erau potrivite pentru includere în MoReq2. Cu toate acestea, calitatea generală a comentariilor a fost extrem de ridicată, şi acesta a condus la o perfecţionare a proiectului anterior.

Aceasta a dus la publicarea versiunii 2 a proiectului, un document complet în liniile esenţiale, pentru ca toate grupurile să poată discuta pe baza lui. La primire, aceste comentarii au fost revăzute şi implementate sau respinse, la fel ca mai sus.

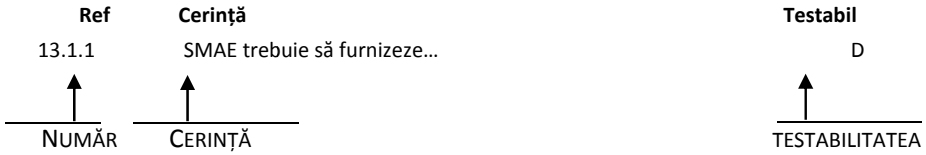
O formă completă a fost întocmită pentru Ofiţerul de proiect al CE şi pentru membrii Forumului DLM pentru revizuire în octombrie 2007. La primirea comentariilor revăzute ale CE, proiectul final al MoReq2 a fost pregătit, care a fost supus revizuirii unui revizor semi-independent înainte de publicarea lui în ianuarie 2008.

Anexa 3 – Folosirea aceste specificaţii în formă electronică

Această specificaţie a fost astfel pregătită încât să poată fi folosită în formă electronică. A fost pregătită folosindu-se Microsoft® Word 2003.

Principalul avantaj al folosirii specificației în formă electronică este că poate fi personalizat cu ușurință.

Cerinţele (de la capitolul al 11) sunt prezentate sub formă de tabele, cu o cerinţă pe rând de table. Aceasta este ilustrată în figura A3.1.



Figură A3.1

Tabelul constă din 3 coloane:

- **Ref:** numărul de referinţă al cerinţei. Aceasta este generată în mod automat de Microsoft Word, deoarece numărul de referinţă as foloseşte un stil de ,,titlu". Rezultatul este că, dacă se vor adăuga sau extrage capitole, secţiuni sau cerinţe, numerotarea se va modifica automat.
- **Cerinţă:**
  - Textul cerinţei:. Acesta foloseşte întotdeauna unul din verbele „trebuie" (pentru a indica o cerinţă obligatorie) or „ar trebui" (pentru a indica o cerinţă recomandabilă);
  - Textul explicaţiei. Acesta este întotdeauna scris cu i*talice*, şi oferă exemple sau o descriere suplimentară a cerinţei.;
- **Test**: fiecare cerinţă este urmată de un atribut numit ,,testabil", prescurtat ,,test". Acesta indică dacă va fi posibilă testarea de conformitate cu cerinţa. Posibilele valori ale atributului ,,testabil" sunt descrise mai jos, cu exemple:
  - D – Cerinţa poate fi testată cu precizie. Un exemplu este „ SMAE trebuie să permită cel puţin trei niveluri ierarhice într-o schemă de clasificare". Aceasta poate fi testată prin încercarea de a realiza o ierarhie cu trei niveluri.
  - N – Cerinţa nu poate fi testată cu precizie. UN exemplu este: „ SMAE trebuie să accepte schema de clasificare a organizaţiei. Nu există nici o posibilitate de a testa această cerinţă pentru toate cazurile.

- P – Cerinţa poate fi testată, dar acoperirea acestui test este parţială sau nu este posibilă o testare precisă, dar este posibil ca o lipsă de conformitate să poată fi descoperită. Un exemplu este: „ SMAE nu ar trebui să limiteze numărul de niveluri în ierarhie”Nu există nici o posibilitate precisă de a testa o absenţă sau o limită. Cu toate acestea, cerinţa este considerată testabilă cu acoperire parţială, de pildă prin testarea pentru un număr mare de niveluri, şi este posibil ca în timpul testării să fie remarcată o limitare a numărului de niveluri, indicându-se astfel că SMAE nu este conform cu cerinţa.

Dacă cerinţe, secţiuni sau capitole unt şterse, Microsoft Word va înlocui orice referinţă încrucişată către acestea (dacă există) cu un mesaj de eroare. Acestea pot fi identificare prin căutarea textului ‚**error!**”

Implicit, liniile tabelului nu sunt vizibile. Acestea pot fi vizualizate prin folosirea comenzii ,,Show gridlines” (,,Arată caroiajul”).

Anexa 4 —Mulțumiri

Echipa de proiect

Mr Frank Brady	European Commission (client)
Mr Tim Burrows	Serco Consulting
Mr Peter Campbell-Burns	Serco Consulting
Mr Keith Cornwell	Serco Consulting
Ms Alayne Crozier	Serco Consulting
Mr Steve Davies	Serco Consulting
Mr John Deverill	Serco Consulting
Mr Marc Fresko	Serco Consulting
Mr Michael Haimerl	Imbus AG (testing partner)
Mr Tilo Linz	Imbus AG (testing partner)
Mr Wasif Mehdi	Serco Consulting
Mr Thomas Rumi	Imbus AG (testing partner)
Mr Josephus Schram	European Commission (Project Officer)
Mr John Seeley	Serco Consulting
Ms Caroline Senior	Serco Consulting
Mr Michael Sill	Imbus AG (testing partner)
Ms Natasha Smith	Serco Consulting

Echipa de proiect doreşte să aducă mulţumirile sale dlui John Worsfold de la Institutul Naţional pentru regal pentru nevăzători (UK) pentru ajutorul dat în scrierea cerinţelor referitoare la accesibilitate.

Colegiul de redacție

Echipa de proiect a fost asistată şi îndrumată de următorul Comitet de redacţie, compus din experţi internţionali.

Mr Miguel Camacho	Sadiel S.A, Spain
Ms Marie-Anne Chabin	Archive 17,France
Ms Anne Mette Dørum	National Archives of Norway, *records management* Department, Norway
Professor Luciana Duranti	School of Library, Archival and Information Studies, University of British Columbia, Canada
Professor Mariella Guercio	University of Urbino, Italy
Mr Peter Horsman	Archiefschool (Netherlands Institute for Archival Education and Research), The Netherlands
Dr Ulrich Kampffmeyer	PROJECT CONSULT Unternehmensberatung GmbH, Germany
Mr Paul Murphy	Ministry of Finance, Ireland

Forumul DLM

Forumul DLM a furnizat un Grup de recenzori pentru a revizui versiunile intermediare în numele Comisiei Europene.

Mr Richard Blake	UK
Ms Dolores Carnicer Arribas	Spain
Mr Olivier de Solan	France
Dr Andrea Hänger	Germany
Ms Paivi Happonen	Finland
Mr Toivo Jullinen	Estonia
Mr Göran Kristiansson	Sweden
Mr Ian MacFarlane	UK
Mr Atle Skjekkeland	Secretariat
Mr Jože Škofljanec	Slovenia
Mr Malcolm Todd (chair)	UK
Mr Martin Waldron	UK

Colaboratori pentru revizuire

Echipa de proiect este extrem de recunoscătoare următoarelor personae şi companii care cu amabilitate s-au oferit voluntari şi au cheltuit o importantă perioadă de timp pentru a participa la revizuire şi validare. Contribuţia lor valoroasă la MoReq2 a asigurat că specificaţia se poate adresa nevoilor unei cât mai largi comunităţi de utilizatori.

Mr Francisco Barbedo	Archives Panel	Instituto dos Arquivos Nacionais/Torre do Tombo, Portugal
Mr. Jan Dalsten Sørensen	Archives Panel	Danish National Archives
Ms Inta Feldmane	Archives Panel	National Archives of Malta
Mr Håkan Lövblad	Archives Panel	Riksarkivet/National Archives, Sweden
Mr. Michal Wanner	Archives Panel	Department of the Archives Administration and *records management*, Czech Republic
Mr Sergey Afanasiev	Specialists Panel	Records Managers Guild, Russia
Ms Phédra Clouner	Specialists Panel	document@work, Belgium
Mr Michiel Gen	Specialists Panel	ARMA International, Belgium
Ms Kimberley Barata	Users Panel	Parliamentary Archives, UK
Ms Kathy Bashaar	Users Panel	PNC Bank, USA
Mr Daniel J Beard	Users Panel	Xerox Corp, USA
Ms Alissa Burger	Users Panel	Rail Corp, Information and *records management*, Australia
Mr Barry Cahill	Users Panel	Nova Scotia Archives &*records management* Department of Tourism Culture & Heritage,Canada
Mr Lluís-Esteve Casellas Serra	Users Panel	Ajuntament de Girona. SGDAP, Spain
Mr Alejandro Delgado Gómez	Users Panel	Servicio de Archivo y Bibliotecas del Ayuntamiento de Cartagena Archivo Municipal parque de Artilleria, Spain
Mr Paul Dodgson	Users Panel	Leicestershire County Council, UK
Ms Susan Em	Users Panel	Royal Pharmaceutical Society of GB
Ms Trish Fallen	Users Panel	Information Management Practitioner, Australia
Ms Lucia Filimon Stefan	Users Panel	Joint Research Centre of the European Commission, Italy

Ms Fiorella Foscarini	Users Panel	European Central Bank, Germany
Ms Alison Gibney	Users Panel	Cimtech, UK
Mr Stefan Gradmann	Users Panel	Universität Hamburg, Germany
Ms Frances Grey	Users Panel	Parliamentary Archives, UK
Mr Harold C Heard Jr.	Users Panel	Citigroup, USA
Ms Sarah Higgins	Users Panel	Digital Curation Centre, University of Edinburgh, UK
Mrs Caroline Ives	Users Panel	Salford City Council, UK
Mr Philip Jones	Users Panel	Staffordshire County Council, UK
Mr Ben Kettell	Users Panel	Cactus Tecnologia, Spain
Ms Natasha Khramtsovsky	Users Panel	Electronic Office Systems, Russia
Mr Stewart Kirkup	Users Panel	Derbyshire County Council, UK
Mr Päivi Laakso	Users Panel	National Agency for Medicines, Finland
Ms Jessica Lila	Users Panel	USA
Mr Stephen Macintosh	Users Panel	Federal Court of Australia
Ms Sònia Oliveras Artau	Users Panel	Ajuntament de Girona. SGDAP, Spain
Mr Matt O'Mara	Users Panel	
Mr Adam Pope	Users Panel	Information Handy Man, UK
Ms Barbara Reed	Users Panel	Recordkeeping Innovation, Australia
Dr David Reeve	Users Panel	Dorset County Council, UK
Ms Maria Reixach Urcola	Users Panel	Ajuntament de Girona. SGDAP, Spain
Mr Jordi Serra Serra	Users Panel	Generalitat de Catalunya, Spain
Ms Deirdre Sharp	Users Panel	Norfolk County Council, UK
Mr Alan Shipman	Users Panel	Group 5 Training, UK
Ms Marija Šimunović	Users Panel	Supreme Court of the Republic of Croatia
Mr Sundeep Vaid	Users Panel	International Fund for Agricultural Development, Italy
Mr Peter Van Garderen	Users Panel	Artefactual Systems, Canada
Mr Willem Vannester	Users Panel	Stadsarchief Antwerpen, Belgium
Mr Gérard Weisz	Users Panel	Sirius Systems, France
Mr Martin Bartonitz	Vendors Panel	SAPERION, Germany
Mr Solomon Barron	Vendors Panel	IBM, UK
Mr Martin Bould	Vendors Panel	ErgoGroup AS, Norway

Mr Reynolds Cahoon	Vendors Panel	Lockheed Martin, USA
Mr Ian Capon	Vendors Panel	Open Text Corporation, UK
Mr Simon Cole	Vendors Panel	Meridio, UK
Mr Jon Garde	Vendors Panel	Objective Corporation, UK
Mr Graham Hadingham	Vendors Panel	FileNet, UK
Mr Joachim Haessler	Vendors Panel	Haessler Information, Germany
Ms Tamara Hoagland	Vendors Panel	EDRM Solutions, USA
Mr Mike Huberty	Vendors Panel	Lockheed Martin, UK
Mr Chris Hughes	Vendors Panel	Tower Software, UK
Dr Gregor Joeris	Vendors Panel	SER Solutions Deutschland, Germany
Mr Volker John	Vendors Panel	SAPERION, Germany
Dr Annegret Kampe	Vendors Panel	Docuware, Germany
Ms Mary Kelly	Vendors Panel	IBM, UK
Mr Andy King	Vendors Panel	Getronics, UK
Ms Karen McKenzie	Vendors Panel	UK Software
Mr Chris Palmer	Vendors Panel	CA, UK
Ms Shaheen Ramdiane	Vendors Panel	Open Text Corporation
Mr Miroslav Širl	Vendors Panel	ICZ, Czech Republic
Mr Andrew Snowden	Vendors Panel	Fujitsu, UK
Mr Dan Taillefer	Vendors Panel	EMC, Canada
Mr Nigel Wood	Vendors Panel	Fabasoft, UK

Mărci comerciale

Toate mărcile comerciale care apar în prezenta specificaţie sunt făcute cunoscute. PRodusele patentate sunt menţionate doar cu scop de exemplificare; includerea lor nu rprezintă nici o formă de promovare. În mod similar, excluderea altor produse nu implică vreo atitudine critică referitoare la aceleaşi produse.

Anexa 5 – Corespondenţa cu alte modele

Această anexă rezumă modul în care modelul de metadata specificat în anexa 9 poate fi legat de:

- ISO 23081 – Metadate pentru acte;
- ISO 15836 – Setul de elemente de metadate Dublin Core.

ISO 23081– Metadata pentru acte

Entităţile care se regăsesc în MoReq2 pot fi echivalate aproximativ cu echivalentul acestora din ISO 23081, astfel:

Entitate MoReq2	Sub-clase de entităţi în ISO 23081
Componentă (*Component)*	--
Act *(Record)*	Piesă *(Item)*
	Secvenţă de tranzacţie *(Transaction sequence)*
Volum *(Volume)*	Dosar *(File/folder)*
sub-dosar *(Sub-file)*	
Dosar *(File)*	
Clasă *(Class)*	Serie *(Series)*
Schema de clasificare *(Classification scheme)*	Arhivă *(Archive)*
--[-]	Arhive *(Archives)*

Aceste echivalări sunt inevitabil aproximative.

Fiecare din elementele de metadate existente în modelul MoReq2 are o denumire care constă din două sau trei părţi (aşa cum este descries în anexa 9.6). Acolo unde este posibil, a doua parte a numelui este preluată din ISO 23081-2, dar unele au fost dezvoltate pentru MoReq2, aşa cum se poate remarca din tabelul următor:

ISO 23081 Metadata Group	2nd part of MoReq2 Element Name	Source of name
Identity	system_identifier	MoReq2
	system_identifier_rendition	MoReq2

ISO 23081 Metadata Group	2nd part of MoReq2 Element Name	Source of name
Description	abstract	ISO 23081
	author	MoReq2
	classification	ISO 23081
	copy_recipient	MoReq2
	counter_signature	MoReq2
	date	MoReq2
	external_identifier	MoReq2
	place	ISO 23081
	recipient	MoReq2
	sender	MoReq2
	title	ISO 23081
Event plan	abstract	MoReq2
	agent	ISO 23081
	date	ISO 23081
	event_description	ISO 23081
	event_trigger	ISO 23081
	period	MoReq2
	reminder	MoReq2
	status	MoReq2
	volume	MoReq2
Event history	abstract	MoReq2
	date	ISO 23081
	disposal_hold	MoReq2
	transfer_or_destroy	ISO 23081
	transferred_to	MoReq2
Use	administrator	MoReq2
	inactive	MoReq2
	language	ISO 23081
	status	MoReq2
	technical_environment	ISO 23081

ISO 23081 Metadata Group	2nd part of MoReq2 Element Name	Source of name
Relation	agent	MoReq2
	applies_to_agent	MoReq2
	applies_to_class	MoReq2
	cross_referenced_to	MoReq2
	disposal_hold	MoReq2
	entity_agent	MoReq2
	has_redaction	MoReq2
	has_role	MoReq2
	has_user	MoReq2
	is_child_of	MoReq2
	is_member_of	MoReq2
	is_redaction_of	MoReq2
	is_parent_of	MoReq2
	previous_fully_qualified_classification_code	MoReq2
	r&d_schedule	MoReq2
	record_type	MoReq2

Alte aspect referitoare la corespondența între MoReq2 și ISO 23081 sunt redate în anexa 9.

ISO 15836 —setul de elemente de metadate Dublin Core

Elementele definite în Dublin Core pot fi echivalate cu elementele din modelul MoReq2, după cum urmează. Acolo unde doar un nume parţial de element MoReq2 este prezentat, el indică toate elementele care încep cu acel nume parţial. Deci, pentru exemplu, Description.abstract indică urmatoarele:

- Description.abstract;
- Description.abstract.keywords;
- Description.abstract.reason_for_rendition

Dublin Core Element	MoReq2 Element
contributor	Description.sender
coverage	-
creator	Description.author
date	Description.date

Dublin Core Element	MoReq2 Element
description	Description.abstract.description Description.external_identifier.internal_reference
format	Use.technical_environment.format Use.technical_environment.file_format
identifier	Identity
language	Use.language
publisher	-
relation	Relation
rights	-
source	-
subject	Description.abstract.keyword
title	Description.title
type	Description.record_type
-	Description.abstract.mandate Description.abstract.reason_for_rendition Description.copy_recipient Description.place.current_location Description.place.home_location Description.recipient Event_history Event_plan Use.status Use.technical_environment (save as above)

De reținut că aceste echivalări sunt inevitabil aproximative.

Alte aspect referitoare la corespondența între MoReq2 și ISO 23081 sunt redate în anexa 9.

Anexa 6—Prelucrarea datei

Se cere ca un SMAE să proceseze toate datele corect, indiferent de mileniu, secol sau altă formă de reprezentare a datei. Această anexă prezintă o declaraţie a cerinţei pentru procesarea problemei „Anul 2000” care ar putea fi adaptată, dacă este ecesar, să se refere şi la alte date. Aceasta va fi în mod particular relevant pentru Sistemele de Management al Actelor Electronice care ar putea include metadate despre date pentru secolele anterioare şi viitoare.

Secţiunea care urmează este reprodusă cuvânt cu cuvânt, cu acord, din BSI DISC PD2000-1:1998 *A Definition of Year 2000 Conformity Requirements* (O definire a cerinţelor de conformitate ,,Anul 2000”).

Conformitatea cu problema ,,Anul 2000” va însemna că nici performanţa şi nici funcţionalitatea nu sunt afectate de datele anterioare, în timpul şi după anul 2000.

În special:

- **Regula 1** Nici o valoare pentru data actuală nu va genera vreo întrerupere în operare.
- **Regula 2** Funcţionalitatea bazată pe dată trebuie să se comporte uniform pentru datele anterioare, din timpul şi după anul 2000.
- **Regula 3** In toate interfeţele şi stocări de date, secolul din orice dată trebuie să fie specificat fie explicit, fie printr-un algoritm sau reguli de inferență neechivoce.
- **Regula 4** Anul 2000 trebuie să fie recunoscut ca an bisect.

Anexa 7 — Standarde și alte linii directoare

7.1. Standarde

Această anexă prezintă standard și alte resurse la care s-a făcut referire în specificație sau care se aplică managementului actelor electronice.

Standardele incluse sunt cele cu relevanţă specială pentru SMAE ; sunt omise standardele generale, cum ar fi cele care tratează dispozitive de stocare şi limbaje de baze de date.

Standardele include standarde internaţionale, atât de jure, cât şi de facto. Standardele naţionale sunt omise din această listă. Acestea pot fi adăugate la Capitolul zero, de către autoritatea specifică unui stat membru. Sunt incluse doar standardele care au o implicare directă în proiectarea sistemelor, nefiind cuprinse standarde care tratează managementul organizării şi al continuităţii. În majoritatea cazurilor, este prezentat numele scurt al standardului (şi nu cel cu toate calificativele), pentru uşurarea înţelegerii.

FIPS 186-2	NIST Digital Signature Standard (http://csrc.nist.gov/publications/PubsFIPS.html)
ISAAR(CPF)	International Standard Archival Authority Record for Corporate Bodies, Persons, and Families (International Council on Archives) (http://www.ica.org/en/node/30230)
ISAD(G)	International Standard for Archival Description (General). (http://www.icacds.org.uk/icacds.htm)
IETF RFC 2821	Simple Mail Transfer Protocol. http://www.ietf.org/rfc/rfc2821.txt)
IETF RFC 2822	Internet Message Format. (http://www.ietf.org/rfc/rfc2822.txt)
ISO 216	Writing paper and certain classes of printed matter – Trimmed sizes – A and B series
ISO 639	Codes for the representation of names of languages.
ISO 2788	Guidelines for the establishment and development of monolingual thesauri.
ISO 5964	Guidelines for the establishment and development of multilingual thesauri.
ISO 8601	Representation of dates and times.

ISO 9834-8	Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components (see also ITU X.667).
ISO/TS 12033	Guidance for selection of document image compression methods.
ISO/TR 12037	Recommendations for the expungement of information recorded on write-once optical media.
ISO 12142	Media error monitoring and reporting techniques for verification of stored data on optical digital data disks.
ISO/TR 12654	Recommendations for the management of electronic recording systems for the recording of documents that may be required as evidence, on WORM optical disk.
ISO 14721	Open archival information system – Reference model (OAIS).
ISO/IEC 15444	JPEG 2000 image coding system: Core coding system.
ISO 15489	*records management*.
ISO/TR 15801	Information stored electronically – Recommendations for trustworthiness and reliability.
ISO 15836	The Dublin Core metadata element set.
ISO 18492/TR	Long-term preservation of electronic document-based information.
ISO 19005-1	Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).
ISO 23081	Metadata for records.
ITU X.667	Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components. (http://www.itu.int/ITU-T/studygroups/com17/oid/X.667-E.pdf).
TIFF	Tagged Image File Format. (http://partners.adobe.com/public/developer/tiff/index.html)
X.509	ITU-T Recommendation X.509: Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. (http://www.itu.int/rec/T-REC-X.509-200003-I/en).
XKMS	XML Key Management Spec. (http://www.w3.org/TR/xkms/).
XML	W3C Extensible Markup Language (XML) (http://www.w3.org/TR/REC-xml/)

7.2. Alte îndrumătoare

ISO/DIS 9241-171	Ergonomics of human-system interaction – Part 171: Guidance on software accessibility
ISO/TS 16071	Guidance on accessibility for human-computer interfaces (due to be superseded by ISO 9241-171).
WfMC	Workflow Management Coalition Terminology & Glossary. (http://www.wfmc.org/standards/referencemodel.htm)
1999/93/EC	Directive on a Community Framework for Electronic Signatures. (http://europa.eu/scadplus/leg/en/lvb/124118.htm)
DLM Forum Guidelines	Guidelines on best practices for using electronic information. INSAR (European Archives News) Supplement III (1997). ISBN: 92-828-2285-0. (http://dlmforum.typepad.com/gdlines.pdf)

7.3. Resurse și linii directoare pentru accesibilitate

Această secțiune enumeră liniile directoare și resursele pentru dezvoltatori și cumpărători de SMAE. În timp ce alte secțiuni ale anexelor conțin doar publicații deschise și internaționale, această secțiune include informații care au fost la origine naționale și care își au originea în comunitatea furnizorilor. Această situație se datorează faptului că nu a fost identificata o documentație acceptată la nivel internațional; aceasta ar putea fi adăugată în edițiile viitoare ale MoReq2.

Pentru dezvoltători
W3C Web Content Accessibility Guidelines (for websites and web applications) (http://www.w3.org/WAI/)
RNIB Web Access Centre (http://www.rnib.org.uk/webaccesscentre)
RNIB Software Access Centre (http://www.rnib.org.uk/softwareaccesscentre)
IBM Human Ability and Accessibility Centre (http://www-03.ibm.com/able/guidelines/)
ISO/IEC 18019 Guidelines for the design and preparation of user documentation for application software (see especially clause 4.2.6). (Due to be replaced by ISO/IEC 26514.)
ISO/IEC 26514 User documentation requirements for documentation designers and developers. (Under development).
Pentru licitații
ACCENT – Accessibility in ICT Procurement: EU project (http://www.verva.se/english/international-network/the-accent-project/)

PAS 78:2006 A guide to good practice in commissioning accessible websites (http://www.equalityhumanrights.com/en/publicationsandresources/Disability/Pages/Websiteaccessibilityguidance.aspx)
RNIB Software Access Centre (http://www.rnib.org.uk/softwareaccesscentre)

7.4. Linii directoare privind prezervarea digitală

InterPARES project (http://www.interpares.org)
Preserving Access to Digital Information (PADI) project National Library of Australia (http://www.nla.gov.au/padi/)
The National Archives Functional Requirements for the Sustainability of Electronic Records (http://www.nationalarchives.gov.uk/documents/functional_requirements.pdf)

7.5. Modelul grafic al relației dintre MoReq2 și alte îndrumătoare

Această secțiune conține un model grafic care prezintă cum standardele esențiale sunt legate de managementul actelor electronice El folosește un nou model de management al actelor electronice, prezentat în figura A7.1, care a fost pregătit special pentru acest scop.

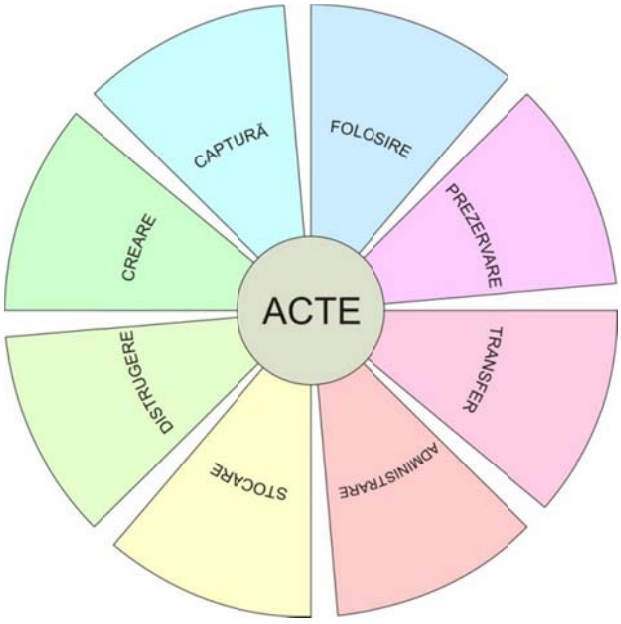


Figura A7.1

Acest model prezintă procesele cheie care afectează actele electronice. Acele sunt reprezentate de cercul central, cenușiu. Prcesele (creare, captură etc.) sunt reprezentate de sectoare de cerc colorate, ce înconjoară actele.

Numărul de procese prezentat (granularitatea sau niveul de detaliere al modelului) este oarecum arbitrar. Câteva alte reprezentări sunt posibile, şi ar fi mai potrivite pentru alte scopuri; cel anterior a fost ales intenţionat pentru a fi pus în legătură cu standardele. Pentru a interpreta aceste procese:

- **Crearea** nu include doar crearea actelor din cadrul unei organizaţii, ci şi primirea actelor din afara organizaţiei.
- **Captura** include înregistrarea, clasificarea şi introducerea metadatelor pentru managementul actelor.
- **Folosirea** include căutarea, regăşirea, parcurgere,redarea, păstrarea, revizuirea etc.
- **Prezervarea** reprezintă procesele cerute pentru menţinerea accesibilităţii în timp.
- **Administrarea** include păstrarea comenzilor de acces şi a autorităţilor de dispoziţie.

Ordinea proceslor prezentate nu este semnificativă, deoarece acestea se pot produce în diferite secvenţe în diferite setări.

Simplificând foarte mult, standardele cheie care se aplică managementul actelor electronice care pot fi puse în legătură cu aceste procese este prezentat în figura A7.2

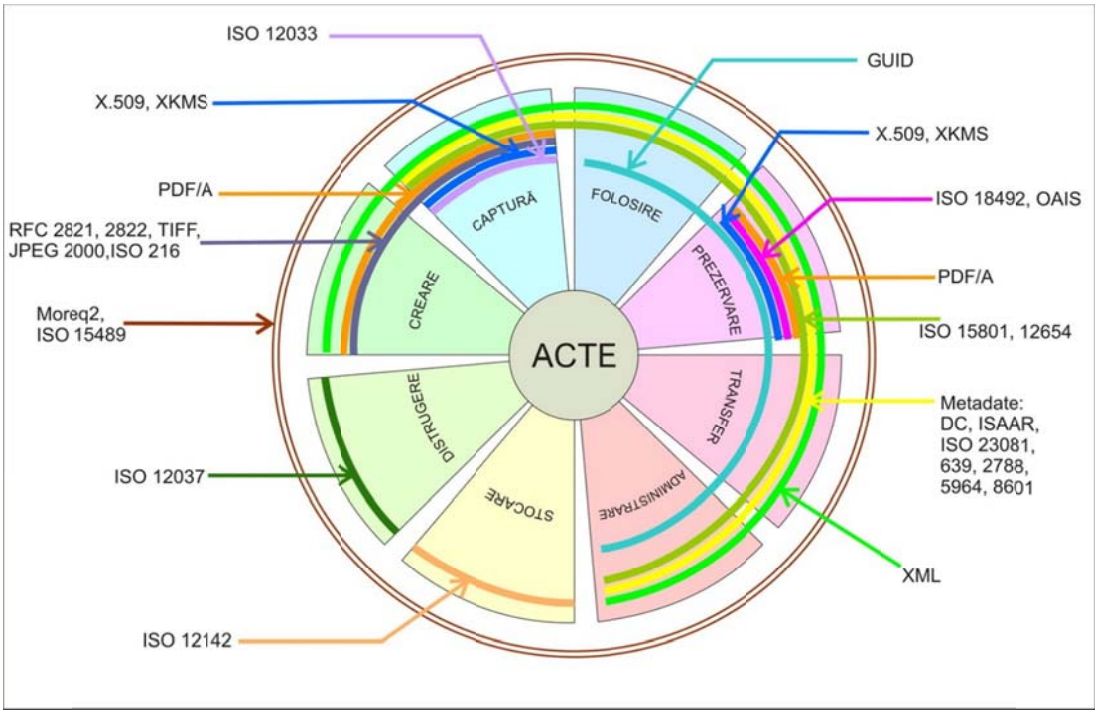


Figura A7.2

Relaţia prezentată mai sus între standarde şi procese se repetă la sfârşitul acestei secţiuniîntr-o formă care nu necesită culoare.

Acest model urmăreşte zona de relevanţă a standardelor –de o manieră foarte aproximativă— folosind linii colorate care se suprapun proceselor. Fiecare linie colorată reprezintă unul sau mai multe standarde. Acolo unde este posibil, standardele au fost denumite cu numele lor obişnuit (de ex. PDF/A, OAIS) şi nu cu numărul lor de standard, mai puţin sugestiv (de ex. ISO 19005, ISO 14721); a se vedea secţiunea 1 a acestei anexe pentru titlurile oficiale. De remarcat că orice model de acest fel nu poate da decât o orientare generală – nu este posibilă furnizarea detaliilor despre interacţiunea proceselor şi standardelor; într-o anumită măsură, includerile şi omiterile reflectă o perspectivă subiectivă.

Doar standardele care sunt considerate ca fiind cele mai importante sunt incluse în diagramă; celelalte sunt excluse. Criteriul pentru includere sau excludere poate fi discutabil.

Modelul este explicat mai jos. Standardele care sunt aplicabile mai multor procese sunt explicate mai jos, urmate de standardele relevante pentru fiecare proces.

ISO 15489 şi MoReq2

ISO 15489 şi MoReq2 acoperă ambele integralitatea proceselor care afectează actele electronice. În consecinţă, ele sunt prezentate ca acoperind toate procesele.

XML

XML este prezentat ca fiind relevant pentru aproape toate procesele – cu excepţia stocării şi distrugerii. Relevanţa sa variază extrem de mult, în funcţie de mediu. Totuşi, în principu, el poate influenţa formatul creării actelor, apoi felul în care metadatele sunt stocate şi exprimate la captură şi în tipul folosirii ulterioare; este un standard important care facilitează innterpretarea metadatelor şi conţinutului în cadrl păstrării pe termen lung; poate fi de asemenea folosit pentru a furniza o schemă comună de transfer între sisteme; poate fi folosit să descrie accesul şi scheme şi autorităţi de dispoziţie.

Metadate

Standardele de metadate sunt relevante pentru procesul de captură, folosire, prezervare, transfer şi administrare. Acestea includ ISO 23081 (care acoperă toate aspectele metadatelor relevante pentru managementul actelor), Dublin Core (care specifică un set standard de metadate pentru descoperire), ISO 639 (vocabular controlat pentru coduri lingvistice), ISAD şi ISAAR (abordări pentru folosirea metadatelor în domeniul creării documentelor şi descriere arhivistică) şi standardele ISO 2788 şi 5984 (standarde referitoare la tezaure).

Crearea

Cel mai important standarde în procesul de creare a actelor este formatul actelor. Există mai multe standarde de format incluzând RFC 2821/2822 (pentru e-mail), ISO 216, TIFF şi JPEG (pentru imagini scanate), şi PDF/A.

Captura

Standardele de metadate de toate felurile se aplică puternic procesului de captură. Unele dintre standardele de format ce influenţează captura sunt de asemenea relevante din punctul de vedere al extragerii automate a valorilor de metadate. Standardele referitoare la aspectele juridice se aplică de asemenea la captură, repectiv ISO 15801 şi ISO 12654.

Folosirea

Standardul care guvernează GUID (numere de identificare unice globale), X.667, influenţează felul în care actele electronice sunt folosite, aşa cum se întâmplă şi cu standardele referitoare la aspecte juridice, ISO 15801 şi ISO 12654.

Prezervare

Standardul esenţial pentru prezervare este OAIS; acesta funizează un cadru pentru proiectarea şi administrara activităţilor de prezervare. ISO 18492 furnizează de asemenea indrumări generale. Majoritatea muncii de prezervare se bazează fundamental pe standardele de metadate, şi unul dintre standardele fundamentale este PDF/A, care descrie un format de prezervare. Standardele pentru semnătură electronică, X.509 şi XKMS au de asemenea implicaţii în problemele de prezervare.

Transfer

Folosirea standardelor de metadate este esenţială pentru transferul între organizaţii sau între sisteme.

Administrare

Standardele de metadate pot sprijini procesele de administrare a accesului şi păstrării. De asemenea, sunt relevante standardele juridice, ISO 15801 şi 12654.

Stocarea

ISO 12142 tratează un aspect special al stocării, referitor la stocarea pe discuri optice.

Distrugerea

ISO 12037 tratează un aspect limitat al distrugerii, respectiv distrugerea (expungement); acesta este relevant doar în anumite medii.

Relaţia între standarde şi procese este prezentată mai jos într-o formă tabelară, care nu necesită culori pentru reprezentare. Acest tabel prezintă procesele în coloane şi standardele în rânduri. Acolo unde un semn de confirmare (?) este prezent la intersecţia între un rând şi o coloană, acesta indică faptul că standardul corespondent este legt de procesul corespunzător.

Standard		Creare	Captură	Folosire	Prezervare	Transfer	Administrare	Stocare	Distrugere
ISAAR(CPF)	International Standard Archival Authority Record for Corporate Bodies, Persons, and Families (International Council on Archives).		☐	☐	☐	☐	☐		
IETF RFC 2821	Simple Mail Transfer Protocol.	☐	☐						
IETF RFC 2822	Internet Message Format.	☐	☐						
ISO 216	Writing paper and certain classes of printed matter – Trimmed sizes – A and B series	☐	☐						
ISO 639	Codes for the representation of names of languages.		☐	☐	☐	☐	☐		
ISO 2788	Guidelines for the establishment and development of monolingual thesauri.		☐	☐	☐	☐	☐		
ISO 5964	Guidelines for the establishment and development of multilingual thesauri.		☐	☐	☐	☐	☐		
ISO 8601	Representation of dates and times.		☐	☐	☐	☐	☐		
ISO 9834-8	Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components (see also ITU X.667).			☐			☐		
ISO 12033	Guidance for selection of document image compression methods.		☐						
ISO 12037	Recommendations for the expungement of information recorded on write-once optical media.								☐

Standard		Creare	Captură	Folosire	Prezervare	Transfer	Administrare	Stocare	Distrugere
ISO 12142	Media error monitoring and reporting techniques for verification of stored data on optical digital data disks.							☑	
ISO 12654	Recommendations for the management of electronic recording systems for the recording of documents that may be required as evidence, on WORM optical disk.		☑	☑			☑		
ISO 14721	Open archival information system – Reference model (OAIS).				☑				
ISO 15444	JPEG 2000 image coding system: Core coding system.	☑	☑						
ISO 15489	*records management*.	☑	☑	☑	☑	☑	☑	☑	☑
ISO 15801	Information stored electronically – Recommendations for trustworthiness and reliability.		☑	☑			☑		
ISO 15836	The Dublin Core metadata element set.		☑	☑	☑	☑	☑		
ISO 18492	Long-term preservation of electronic document-based information.				☑				
ISO 19005-1	Electronic document file format for long-term preservation.	☑	☑		☑				
ISO 23081	Metadata for records.		☑	☑	☑	☑	☑		
ITU X.667	Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components.			☑			☑		
MoReq2	Update and extension of the Model Requirements for the management of electronic records	☑	☑	☑	☑	☑	☑	☑	☑

Standard		Creare	Captură	Folosire	Prezervare	Transfer	Administrare	Stocare	Distrugere
TIFF	Tagged Image File Format.	☐	☐						
X.509	ITU-T Recommendation X.509: Open systems interconnection – The Directory: Public-key and attribute certificate frameworks.		☐		☐				
XKMS	XML Key Management Specification.		☐		☐				
XML	W3C Extensible Markup Language.	☐	☐	☐	☐	☐	☐		

Anexa 8 — Modificări față de versiunea anterioară

8.1.Modificări incompatibile cu versiunea anterioară

MoReq2 a fost scris pentru a asigura, în măsura posibilului, compatibilitatea cu MoReq original. Inovația majoră din această ediție este stocarea actelor direct în clase, fără a mai folosi dosare. Această situație este tratată în secțiunea 3.2; trebuie observat că SMAE poate fi configurat să dezactiveze această opțiune.

Posibilitatea de a crea atât sub-dosare, cât și volume în cadrul dosarelor este de asemenea nouă în MoReq2 (vezi secțiunea 3.3). Aceasta nu ridică nici o problemă de compatibilitate cu ediția precedentă, dar este o nouă cerință majoră.

De asemenea, definițiile prezentării și redării au fost inversate față de definiția din versiunea anterioară a MoReq. Vezi glosarul pentru o definiție completă a ambilor termeni.

8.2. Relații între secțiuni

Structura MoReq2este reflectată în MoReq2, cu unele modificări și câteva adăugiri. Această secțiune marchează corespondența între secțiuni în MoReq2și MoReq2.

MoReq2		MoReq2	
Cap.	**Titlu**	**Cap.**	**Titlu**
	Preface		Preface: MoReq2
1	Introduction	1	Introduction
1.1	Background	1.1	Background
1.2	Purpose and Scope of this Specification	1.3	Purpose and Scope of this Specification
1.3	What is an SMAE ?	1.4	What is an SMAE ?
1.4	For What can this Specification be Used?	1.5	For what can this Specification be used?
1.5	Emphasis and Limitations of this Specification	1.7	Emphasis and Limitations of this Specification
1.6	Using this Specification	1.9	Customising this Specification
1.7	Organisation of this Specification	1.10	Organisation of this Specification
1.8	Mandatory and Desirable Requirements	1.12	Mandatory and Desirable Requirements
1.9	Intellectual Property	1.6	Intellectual property rights
2	Overview of SMAE Requirements	2	Overview of SMAE Requirements

MoReq2		MoReq2	
Cap.	**Titlu**	**Cap.**	**Titlu**
2.1	Key Terminology	2.1	Key Terminology
2.2	Key Concepts	2.2	Key Concepts
2.3	Entity-Relationship Model	2.3	Entity-Relationship Model
3	Classification Scheme	3	Classification Scheme and File Organisation
3.1	Configuring the Classification Scheme	3.1	Configuring the Classification Scheme
3.2	Classes and Files	3.2	Classes and Files
3.3	Volumes	3.3	Volumes and Sub-Files
3.4	Maintaining the Classification Scheme	3.4	Maintaining the Classification Scheme
4	Controls and Security	4	Controls and Security
4.1	Access	4.1	Access
4.2	Audit trails	4.2	Audit trails
4.3	Backup and Recovery	4.3	Backup and Recovery
4.4	Tracking Record Movements		Deleted (covered in section 10.1)
4.5	Authenticity		Deleted (covered in chapter 2)
4.6	Security Categories	10.15	Security Categories
5	Retention and Disposal	5	Retention and Disposition
5.1	Retention Schedules	5.1	Retention and Disposition Schedules
5.2	Review	5.2	Review of Disposition Actions
5.3	Transfer, Export and Destruction	5.3	Transfer, Export and Destruction
6	Capturing Records	6	Capturing and Declaring Records
6.1	Capture	6.1	Capture
6.2	Bulk importing	6.2	Bulk Importing
6.3	Types of Document		Deleted (covered in section 6.1)
6.4	E-mail Management	6.3	e-Mail Management
7	Referencing	7	Referencing
8	Searching, Retrieval and Rendering	8	Searching, Retrieval and Presentation
8.1	Search and Retrieval	8.1	Search and Retrieval
8.2	Rendering: Displaying Records	8.2	Presentation: Displaying Records
8.3	Rendering: Printing	8.3	Presentation: Printing
8.4	Rendering: Other	8.4	Presentation: Other
9	Administrative Functions	9	Administrative Functions
9.1	General Administration	9.1	General Administration
9.2	Reporting	9.2	Reporting
9.3	Changing, Deleting and Redacting Records	9.3	Changing, Deleting and Redacting Records
10	Other Functionality	10	Optional Modules
10.1	Management of Non-electronic Records	10.1	Management of Physical (Non-electronic) Files and Records

MoReq2		MoReq2	
Cap.	**Titlu**	**Cap.**	**Titlu**
10.2	Hybrid File Retention and Disposal	10.2	Disposition of Physical Records
10.3	Document Management	10.3	Document Management and Collaborative Working
10.4	Workflow	10.4	Workflow
10.5	Digital Signatures	10.7	Electronic Signatures
10.6	Encryption	10.8	Encryption
10.7	Electronic Watermarks etc.	10.9	Digital Rights Management
10.8	Interoperability and Openness		Deleted (covered in chapters 5, 6 and 10.6)
11	Non-Functional Requirements	11	Non-Functional Requirements
11.1	Ease of Use	11.1	Ease of Use
11.2	Performance and Scalability	11.2	Performance and Scalability
11.3	System Availability	11.3	System Availability
11.4	Technical Standards	11.4	Technical Standards
11.5	Legislative and Regulatory Requirements	11.5	Legislative and Regulatory Requirements
11.6	Outsourcing and Third Party Management of Data	11.6	Outsourcing and Third Party Management of Data
11.7	Long Term Preservation and Technology Obsolescence	11.7	Long Term Preservation and Technology Obsolescence
12	Metadata Requirements	12	Metadata Requirements
12.1	Principles	12.1	Principles
12.2	Organisation of the Remainder of this Chapter	App. 9.1	Introduction
12.3	Classification Scheme Metadata Elements	App. 9.7.1	Classification Schemes
12.4	Class and Electronic File Metadata Elements	App. 9.7.2	Classes, Files, Sub-Files, Volumes
12.5	Metadata Elements for Electronic File or Electronic File Volume	App. 9.7.2	Classes, Files, Sub-Files, Volumes
12.6	Electronic Volume Metadata Elements	App. 9.7.2	Classes, Files, Sub-Files, Volumes
12.7	Record Metadata Elements	App. 9.7.2	Classes, Files, Sub-Files, Volumes
12.8	Record Extract Metadata Elements	App. 9.7.3	Record Redactions
12.9	User Metadata Elements	App. 9.7.8	Agents (Users, Groups and Roles)
12.10	Role Metadata Elements	App. 9.7.8	Agents (Users, Groups and Roles)
12.11	Customisation Notes for Metadata Requirements	App. 9.9	Customisation Notes for Metadata Requirements
13	Reference Model	13	Reference Model
13.1	Glossary	13.1	Glossary
13.2	Entity-Relationship Model	13.2	Entity-Relationship Model
13.3	Entity-Relationship Diagram Narrative	13.3	Entity-Relationship Narrative

MoReq2		MoReq2	
Cap.	**Titlu**	**Cap.**	**Titlu**
13.4	Access Control Model	13.4	Access Control Model
	ANNEXES		APPENDICES
Ann. 1	Reference Publications	App. 1	Reference Publications
Ann. 2	Development of this Specification	App. 2	Development of this Specification
Ann. 3	Use of this Specification in Electronic Form	App. 3	Use of this Specification in Electronic Form
Ann. 4	Acknowledgements	App. 4	Acknowledgements
1	Project Team	App. 4.1 App. 4.2	Project Team Editorial Board
2	Validation Organisations	App. 4.3 App. 4.4	DLM Forum Review Panellists
3	Trademarks	App. 4.5	Trademarks
Ann. 5	Correspondence to Other Models	App. 5	Correspondence to Other Models
1	Correspondence to Dublin Core Metadata Model	App. 5.2	ISO15836 – The Dublin Core metadata standard
2	Correspondence to Pittsburgh metadata model	—	—
Ann. 6	Date Processing	App. 6	Date Processing
Ann. 7	Standards and Other Guidelines	App. 7	Standards and Other Guidelines
1	Standards	App. 7.1	Standards
2	Other Guidelines	App. 7.2	Other Guidance
3	Accessibility Guidelines	App. 7.3	Accessibility Guidelines and resources
4	Long Term Preservation Guidelines	App. 7.4	Digital Preservation Guidelines

Anexa 9 —Modelul de metadate

Anexa 9 conține modelul de metadate MoReq2. Din cauza dimensiunii textului și pentru a ușura referința încrucișată, este publicată doar în format electronic, la www.dlm-network.org/MoReq2.

MoReq2 – MoReq Governance Board Approval

Name Marko Lukičić

Title Translation & Ch“0“ Workgroup Leader

Signature 

Date 13th February 2012

Name Simon Cole

Title Acting Chair of the MGB

Signature 

Date 13th February 2012

Pagină lăsată intenționat albă

Pagină lăsată intenționat albă

ISBN 978-973-0-12530-6

SPECIFICAȚIA MoReq 2

CERINȚE MODEL PENTRU MANAGEMENTUL ACTELOR ELECTRONICE

2008

FEDERAȚIA ARHIVIȘTILOR DIN ROMÂNIA