NOARK-4

Norwegian recordkeeping system
Version 4

PART I:

Functional description
and specification of requirements

Riksarkivet - The National Archives of Norway,1999
English version 2000

CONTENTS

NOARK-4, PART II: TECHNICAL SPECIFICATIONS

with the chapters listed below have not been translated:

1. INTRODUCTION

1.1 What is Noark-4?

Noark-4 is a specification of functional requirements for electronic recordkeeping systems used in public administration (in Norway). The specification lists requirements with regard to *information content* (what kind of information it should be possible to register and retrieve), *data structure* (design of each data element and the relationship between these elements) and *functionality* (the functions which the systems are to maintain). In some cases there are requirements with regard to the *user interface* (how the systems communicate with the users), but this is mainly left to the individual system developers or vendors to decide. The specification does not contain requirements with regard to the how the data structure is to be implemented, or with regard to system design. This is left to the system developers.

Noark-4 is a revision of the *Noark standard* "Norsk arkivsystem" (Norwegian record-keeping system) of the Norwegian state administration, which was first introduced in 1984 and has since run through several revisions, the previous one being the Noark-3 of 1994[1]. Noark-4 also elaborates the specifications of *Koark*, which is the corresponding standard for local and regional administration. The Koark report[2], published in 1995, essentially follows the same principles as the Noark standard, but includes some additional functions which are specifically adapted to the process of decision-making in Norwegian local and regional administration. The report assumed that Koark would later be incorporated in a common standard for the whole of Norwegian public administration, and this has been accomplished through Noark-4.

As the name suggests, Noark-4 is the fourth version of the Noark standard. It is an updated and modernized version of Noark-3 and Koark, while at the same time being substantially more comprehensive and complex than its predecessors. There is much new functionality in Noark-4, and in many areas the specifications have been more systematically implemented than in previous versions. The design of Noark-4 is based, among other things, on the following:

- Noark- and Koark-based systems have a very large and heterogeneous group of users comprising practically everybody within the Norwegian public administration. In connection with Noark-4, users have voiced many wishes and suggestions calling for enhanced functionality as compared with Noark-3 and Koark. The suggestions all point towards making Noark-4 a more comprehensive and complete information system for those functions that deal with records management and document flow.

[1] Noark-3. Standardsystem for edb-basert journalsystem i statsforvaltningen. Samlet kravspesifikasjon [Standardized system of computerized records management system for the state administration. Complete specification of requirements]. Riksarkivet [National Archives of Norway] 1994.
[2] Koark. Kommunal standard for edb-baserte sak-/arkivsystemer [Municipal standard of computerized records management systems]. Kommunenes sentralforbund [Norwegian Association of Local and Regional Authorities]1995.

- Technological progress (e.g. in terms of processing capacity, storage capacity, window technique, network technology) makes it possible to fulfil more user wishes within a realistic technological framework, without the system becoming too hard to handle or too complex.
- Previous specifications have to a large extent concentrated on *registering and keeping track of* documents (recordkeeping/records management), while *electronic storage* of documents (electronic records) have only been described at a general level. The opportunities of technology and the needs of the users now suggest that the time is ripe for specifying a completely electronic recordkeeping system, where both the registered information and the documents are in electronic form. The work on Noark-4 has shown that a whole new set of requirements are being posed with regard to functionality, interaction between people involved and quality control when it is assumed that all information exists in electronic form only.
- The use of e-mail has exploded in recent years, and e-mail is probably used more and more even for documents in a legal sense being received or dispatched on behalf of organizations or enterprises. A major issue in Noark-4 has been to facilitate the capturing and filing of any e-mail that makes up or contains administration documents. Integration with e-mail are related to and presupposes the solutions for electronic records management discussed in the previous indent.
- An electronic recordkeeping system can stand on its own feet, as the Noark systems have largely done up to now, but the system can be used more efficiently if it is more closely integrated with the document flow. This has to some degree been achieved with Koark for that part of the document flow which concerns political bodies (boards), but such integration may be taken much further. The recordkeeping system ought to be perceived as an integrated part of the worktool for executive officers within public administration. The system should be able to import and store information and documents from the executive functions, and it should be possible to search for information in the records database and distribute this information to all the users. Noark-4 is described with a view to such integration, and attention has been paid to the requirements of the new edition of «Statens generelle kravspesifikasjoner for elektronisk saksbehandling» (SGK)[3].

Noark-4 is described here as a specification of a *system.* This means that the specification should form the basis for the development of an independent system which maintains the records management functions of a public body. If, on the other hand, one wishes to integrate this recordkeeping system in a wider context, such as a case handling system according to the SGK specifications, Noark-4 may be implemented as a *set of functions* or a *module* within this system. However, this presupposes that the Noark functions in such systems are explicitly identifiable, and the requirements specified have the same validity within the framework of a wider system.

1.2 The project work of Noark-4

The framework of the project was defined in note 06.12.96 from Riksarkivet (the National Archives). An agreement had been reached with Kommunenes sentralforbund (KS; the

[3] Elektronisk saksbehandling. Statens generelle kravspesifikasjon [Electronic case handling. General specification of requirements for the state administration]. Statskonsult 1997.

Norwegian Association of Local and Regional Authorities) to incorporate the Koark specifications in a common Noark standard for state and local administration. In a letter of 31.01.97 to the Ministry of Cultural Affairs, the National Archivist (who is also the director general of the National Archives) presented a plan for the implementation of the project. The Ministry of Cultural Affairs has supported this scheme, also in terms of financing.

The *project group* was appointed in a letter of 24.03.97 from the director general. The following people have been members of the group:

Ivar Fonnes, *Riksarkivet [National Archives], leader of the project group*

Steinar Abrahamsen, *Interkommunalt arkiv i Rogaland [Intermunicipal Archives of Rogaland] (appointed by Kommunenes sentralforbund [Norwegian Association of Local and Regional Authorities])*

Katarina de Brisis, *Statskonsult, later Arbeids- og administrasjonsdepartementet [Ministry of Labour and Government Administration] (appointed by Planleggings- og samordningsdepartementet [Ministry of Planning and Coordination])*

Ole Gausdal, *Kommunaldepartementet [Ministry of Local Government], later Næringsdepartementet [Ministry of Industry] (appointed by Arkivledergruppen for departementene [the group of records managers in the state administration])*

Torbjørn Nystadnes, *KITH AS, hired as a consultant*

Trond Sirevåg, *Riksarkivet [National Archives], secretary of the project group*

Jon Atle Haugen, Riksarkivet*[National Archives], member of the project group from January 1998*

After consultation with the Ministry of Cultural Affairs, a reference group was set up, composed of representatives of Statsministerens kontor [Office of the Prime Minister], Kulturdepartementet [Ministry of Cultural Affairs], Planleggings- og samordnings-departementet [Ministry of Planning and Coordination], Justisdepartementet [Ministry of Justice], Kommunenes sentralforbund [Norwegian Association of Local and Regional Authorities], local archives, Norsk Presseforbund [Norwegian Press Association], Norsk arkivråd, the state archives and selected Noark/Koark vendors. The following people have been members of the *reference group*:

Kirsten Ambjørnsen, *Statens Datasentral*

Anna-Brita Bakken, *Buskerud fylkeskommune [Buskerud county council]*

Helene Brynildsen, *Cinet*

Ingvar Engen, *Kulturdepartementet [Ministry of Cultural Affairs]*

Knut-Erik Gudim, *Siemens-Nixdorf Informasjonssystemer*

Arne Jensen, *Norsk Presseforbund [Norwegian Press Association]*

Thor Kristoffersen, *Justisdepartementet [Ministry of Justice]*

Guro Lysberg, *Telenor Allianse*

Marie Manshaus, *Rogaland fylkeskommune [Rogaland county council]*

Ragnhild Monsen, *Miljøverndepartementet [Ministry of the Environment]*

Jens Nørve, *Planleggings- og samordningsdepartementet [Ministry of Planning and Coordination]*

Kari Remseth, *Statsarkivet i Trondheim [Regional State Archives in Trondheim]*

Arne Spildo, *Statsministerens kontor [Office of the Prime Minister]*

Ragnar Sturtzel, *IBM*

Henning Søndergaard, *Oslo byarkiv [City Archives of Oslo]*

The reference group has met twice. In addition, a follow-up meeting has been arranged for the vendor members of the group.

Torbjørn Nystadnes of KITH AS has been hired as a consultant and planner throughout the project work. In the autumn of 1997, Ove Jordbakke and Ellen Strålberg Janson of ECsoft AS were hired to do writing work. Towards the end of the project period, in the autumn of 1998, Anne Mette Dørum of Forvaltningsinfo AS was hired to compare comments and contribute to the completion of the writing work.

The project group had its first meeting on 4 April 1997. The original project plan aimed at finishing the work with a version of Noark-4 to be circulated for comments in December 1997. The work was somewhat delayed, among other reasons because the specifications were more comprehensive than had been anticipated. The version to be circulated for comments was ready by June 1998. It was published on the Internet and sent to a number of state and local bodies for comments, the deadline being 15 September. 53 opinions were received, and during the autumn of 1998 a number of adjustments were made and definitions incorporated based on comments received.

The work of the project group has taken the form of internal reports and lengthy work meetings. Altogether, the group has met 14 times.

In its work, the project group has made a point of communicating with a number of people about questions relating to the way Offentlighetsloven [the Freedom of Information Act] is being used. A number of meetings have been arranged with representatives of the Ministry of Justice and Norsk presseforbund [Norwegian Press Association].

Furthermore, it has been deemed important to coordinate the specifications of Noark and SGK. For this purpose, meetings were arranged between Statskonsult, the Ministry of Cultural Affairs and the National Archives at the start of the Noark project work. Coordination has also been sought by having staff from Statskonsult (de Brisis) and the National Archives (Sirevåg) as members of both the SGK project group and the Noark project group.

The project has drawn on a wealth of experience from Noark/Koark users and vendors.

The adaption of the material after the round of comments has mainly been carried out by the project managers in co-operation with the hired consultants Torbjørn Nystadnes and Anne Mette Dørum.

1.3 The design of the report

As previously mentioned, Noark-4 is a revision of previous versions of the Noark standard as well as Koark. This leaves an imprint on the report in the form of references to previous solutions as well as discussions on changes in comparison with Noark-3 and Koark. At the same time, Noark-4 is intended to be a report that can stand on its own feet. Reading this report should be sufficient to grasp what is entailed in the new version of the Noark standard and to develop systems based on Noark-4.

The report is primarily aimed at two groups of users:

- System vendors wishing to develop Noark systems for public administration
- Administrative bodies and other institutions that use or plan to use a Noark system

For the system vendors, the report is meant to be a worktool during system development. Much work has gone into systematizing and formalizing the requirement specifications, so that it is easy to find out what are requirements, on what level the requirements are, and what are merely recommendations or suggestions. Chapter 1.4 gives a complete overview of the requirement structure of Noark-4.

Unlike earlier reports, Noark-4 includes a comprehensive technical specification where all attributes which are discussed in the report, are described. This is primarily meant as a guide for system developers, and it is stated several places that the technical implementation does not have to follow these specifications as long as the requirements are otherwise satisfied. However, many of the attributes are a mandatory part of a Noark system, both in terms of existence and design.

For existing and potential users, the report is meant to give an overview of what is contained in a Noark system and what is new in Noark-4 compared with to previous specifications. This would be particularly useful in connection with evaluation, selection and implementation of a new system, or a new version of an existing system. The report may, however, also be useful during reviews of administrative routines, outsourcing and periodization of records as well as transfer of records to an archival repository.

1.3.1 Main structure

The report has two main parts:

Part I: Functional description and specification of requirements
First a general introduction to Noark-4 is given, where the recordkeeping system is placed in context with the recordkeeping and executive functions. Then follows a comprehensive presentation of the standard both at general and detailed levels. The presentation is in the form of a functional description which is closely linked to corresponding procedures and routines. Formalized requirements are given for the individual functions, and these constitute the specification of functional requirements of Noark-4. The presentation includes:

- general description and functional requirements
- main structure of the data model
- purpose, design and functional requirements for the various parts of the system (modules)

- main tables and their information contents (details: see list of attributes in part II)
- assumptions related to administrative routines
- reports and statistics
- integration with e-mail and executive functions
- deviations from Noark-3 and Koark

Part II: Specification of technical requirements
This gives a complete technical specification of the information contents and data structure of Noark-4. The specification takes the form of

- data models for the individual modules
- a complete list of attributes for all tables, associated with individual modules

The data structure in the shape of modules and tables are only guidelines; their purpose is to describe how a Noark system may be implemented to satisfy the functional requirements of part I. The attributes, on the other hand, are part of the specification of requirements (see chapter 1.4). In addition, the following are specified:

- requirements for exchange and export formats
- deviations from Noark-3 and Koark with suggested principles for converting

Part II, together with the formalized functional requirements of part I, should be the frame of reference for the development of a system based on Noark-4. However, it is essential that system developers also familiarize themselves with the description in part I, so that they understand the meaning of the various requirements and the context which they are part of.

For the users it will normally suffice to read part I, but those who seek more detailed information on information content and data structure should turn to the list of attributes in part II. The same applies to those who wish to check to what degree a system conforms to the requirements of Noark-4.

The numbering of the chapters runs throughout the entire report. Thus, part I contains chapters 1 - 12, whereas part II contains chapters 13 - 17. Due to the comprehensive technical specifications, the report has been split into two volumes, one each for parts I and II.

1.3.2 Form of description and terminology

In the specification of information content and data structure, a simplified version of the principles in the so-called E-R model ("entity-relationship") is used. The entities in the data model are referred to as *tables* (corresponding to the concept of "entity" in the E-R model). The *table* concept has been chosen because it is easy to understand intuitively for those who are not specialists in data modelling, and because it is often natural to implement a table in the data model as a table in the data base. It should be noted, however, that the specification does not make specific *requirements* in terms of how the tables of the model should be implemented. This is left to the individual developer/vendor to decide.

The concept of *attribute* is used to represent the various pieces of information that can be included in a table. In normal usage, this is the same as a *field* in a table. An attribute may be assigned different *values*, which in effect constitute the pieces of information that are entered.

> *Example:* The table *Case* contains, among other things, the attribute *Case date*, which may be assigned the value *12.11.1997*.

The description of records management and executive functions uses ordinary scientific terminology, which in most cases is considered part of the normal language. However, sometimes terms are used which must be further explained. This applies, in particular, to those cases where Noark-4 introduces new terms, or where established terms are used in a different or restricted meaning.

A terminology list has been compiled which contains definitions of words and phrases that may be assumed to be unknown, or that need to be precisely defined. This list has been printed as an appendix to both volumes of the report.

1.4 Requirement structure of Noark-4

Systems that are to conform to the requirements of Noark-4, must relate to the following specifications:

- formalized functional requirements in part I (chapters 3 - 12)
- modules, tables and attributes in part II (chapter 14)
- exchange and export formats in part II (chapter 15)

1.4.1 Formalized functional requirements

All the functionality that is described in this report, is not meant to be implemented in every Noark system. It must be possible to realize Noark-4 on various levels depending on the needs of the users. For this purpose, the functional requirements are grouped according to what area the function covers. Each area is indicated by a letter:

O	Obligatory basic version; must be satisfied for the system to be Noark-4 compliant
E	Basic version for functionality related to integrated e-mail
S	Basic version for functionality related to integration with case handling
U	Basic version for functionality related to board handling

If the letters stand on their own, as above, they refer to the lowest level -- the basic level. Noark-4 in its simplest version would only contain O requirements. These O requirements cover only the records management system itself and are obligatory in the sense that they must be part of any Noark solution. If the O requirements are combined with U requirements, the two together would constitute a simple Koark version. This may again be combined with E and S requirements as necessary.

The requirements within each of the four main areas may be expanded with more advanced requirements. These additional requirements constitute separate requirement levels. The levels are hierachically structured and are indicated by the letters cited above followed by a number. Requirements at a higher level must include all requirements at the level below.

The recordkeeping system in a strict sense (the O requirements) have two additional levels, and a number of recommendations are specified:

O1	Extended version; more advanced functionality, but without electronic records
O2	Full version; advanced functionality, and with electronic records
A	Recommendations

The recommendations are, strictly speaking, not requirements in themselves, and they may be applied both to the basic version and on the higher levels. Many recommendations will probably be difficult to implement in a sensible way without considering a specific level, but such conditions will often be self-evident and so are not always mentioned explicitly in the text.

The other three areas, integrated e-mail, case handling and board handling, have only one additional level, and here too recommendations have been included:

E1	Advanced functionality related to integrated e-mail
S1	Advanced functionality related to integration with case handling
U1	Advanced functionality related to board handling
A	Recommendations

All the functional requirements are presented in separate tables, requirement tables, which are integrated in the texts of the various chapters. The requirement tables have three columns: requirement number, text and requirement type/level. Following is an example of such a table, taken from chapter 8:

K8.70	When registering an access code for a registry entry, one should check off for screening of information related to that registry entry, and for electronic documents related to the registry entry (see ch. 8.61 and ch. 8.62).	O
K8.71	When a registry entry has several senders or addressees, these should be screened individually, but collective checking should also be provided for.	O1
K8.72	Screening of registered electronic documents should always be performed from a registry entry with which they are associated. It should be possible to register an access code for the registry entry when associated documents are to be screened, without any of the record information being checked off for screening (see screening code 1 of Noark-3 and Koark).	O2

1.4.2 Modules, tables and attributes

Part I does not give a complete description of all requirements and conditions. To grasp all the details regarding the functionality of the system, it is necessary to read part II as well. Part II shows an example of how all the tables and attributes in a Noark system could be designed. It should be stressed that this is only an example, and that vendors are free to model their systems in an appropriate way, as long as all obligatory attributes are included and the functionality of the attributes is maintained.

The data model in part II is based on the most advanced level, and all the recommendations are included. The list of attributes in part II contains a column K which specifies requirement type (O, O1, O2, etc.) for the individual attributes (see ch. 14.1.1).

The list of attributes also specifies unique abbreviated names for all the attributes. Use of these abbreviated names are obligatory during export (see below), but the system itself may be realized with other attribute names.

To develop a basic solution (requirement type O), it is not necessary to implement all the relations in the data model. For instance, it is perfectly possible to develop a basic version without a 1:M relationship between case and filing plan code, or between registry entry and sender/addressee.

1.4.3 Exchange and export formats

An absolute requirement is that all Noark systems should be able to export data in a uniform way, irrespective of the level at which they are implemented. This format is based on SGML syntax and is further described in chapter 15.3. During export, each attribute should be tagged with the unique field name specified in the list of attributes. Requirements in terms of formats specified in the list of attributes (such as YYYYMMDD for date fields) must also be complied with.

All attributes that are to be included during export for transfer to an archival depository, are marked with the letter «a» in column K in the list of attributes.

Example:
If the system is designed so that *File Code* and *Secondary Code* are registered in separate fields in the assembly of records which constitutes a case (as is done in Noark-3 today), it must be possible to export the contents of the two fields as rows in the table *Filing plan code*.

Chapter 15.4 describes how reports are exported, and even the basic version must be able to export reports -- such as reports from public administration -- in this format.

1.4.4 Summary of minimum requirements and possible combinations

In order for a system to satisfy the minimum requirements of Noark-4, it must

- satisfy all formalized functional requirements of type **O** without a trailing number in part I (chapters 3 - 12)
- include all attributes with requirement type **O** in the list of attributes (chapter 14) and satisfy the functional requirements associated with them
- be able to export all attributes included in the system except those which are set in italics under requirement type in the list of attributes (chapter 14), and also use the export format specified in chapter 15.3
- be able to export electronic reports according to the specifications in chapter 15.4

These are the requirements of the basic version of Noark-4. For enhanced functionality, the following combinations are likely to represent the relevant alternatives for governmental and municipal agencies:

- O + U : Noark-4 version of Koark
- O1 : Enhanced version of registration and records management system
- O1 + U : Enhanced Koark version
- O2 : Electronic recordkeeping system
- O2 + U : Electronic recordkeeping system with board handling
- O2 + S : Electronic recordkeeping system integrated with case handling
- O2 + E : Electronic recordkeeping system integrated with external e-mail

On top level, several types of functionality may be combined:

- O2 + S + E
- O2 + S + U
- O2 + E + U
- O2 + S + E + U

In addition, functions in E, S and U may be supplied with more advanced additional functions from E1, S1 and U1.

Additional recommended functionality (**A**) may be included at levels where the function in question is relevant.

2. FUNCTIONS AND CONTEXT OF THE RECORDKEEPING SYSTEM

As the name suggests, a recordkeeping system is a tool for maintaining the recordkeeping function of an organization. In the case of Noark, this means the recordkeeping function of public administration; thus, the specifications must be adapted to the rules and requirements that apply to that sector. This chapter deals with some of the elements of the public-sector recordkeeping function that determine the design of the recordkeeping system.

The recordkeeping function of public administration is closely associated with the executive function. The registry keeps the documentation of and for the executive function, and there is a continuous document flow between the registry and the executive officers. The recordkeeping system must function within the framework of this interaction, so it is necessary to view it in such a context and consider its relationship with electronic case handling systems. The interface between the specifications of Noark and SGK is a central element in this description.

2.1 How it relates to the recordkeeping function of public administration

The recordkeeping function of public administration consists in keeping track of documents that relate to cases (case documents), placing those documents in their proper context (cases), distributing documents to the executive function, following up the executive function, storing documents that have been processed, responding to internal and external inquiries about the processing status and contents of documents, searching for and retrieving documents upon request, lending out documents or distributing copies, etc. Furthermore, the stored material should after a number of years be transferred to an archival repository as documentation of the activities which caused it to be produced.

The recordkeeping system should be a working tool for all parts of the recordkeeping function. It is used on the one hand to register and store documents and other information, on the other hand to search for and retrieve such information and distribute it. The system must of course be designed so that it covers the tasks that make up the recordkeeping function, as well as possible. At the same time, attention must be paid to the basic framework imposed by laws and regulations, including the definition of what types of documents the records should include. Furthermore, the system must provide for satisfactory quality control in the recordkeeping function.

2.1.1 Laws, regulations and administrative provisions

The recordkeeping function of public administration has for a long time been regulated through a separate set of provisions and regulations. For the state administration, these regulations have been fairly extensive, while local and regional administration have been subject to a less extensive set of regulations. This inequality is about to be levelled out by

the Archives Act ("arkivloven"[4]) and its regulation ("arkivforskriften"), which stipulate common rules for the entire public sector, except rules concerning transfer to archival repository. The Archives Regulation circulated for comments during the summer of 1998, and there is reason to believe that the new act and its regulation will enter into force approximately at the time when Noark-4 is ready for publishing.

The Archives Act and the Archives Regulation will essentially perpetuate, in an updated and modernized form, the current provisions for the state administration. The purpose of the regulation is to ensure the documentation of the commitments and decisions of the administration -- partly for administrative and legal purposes, partly for the knowledge and research of posterity. Essential provisions deal with issues such as the duty to keep records, the organization of the records, what kind of material should be in the records, what should be kept for posterity and how it should be kept. There are also rather detailed provisions regarding recordkeeping procedures, related to document handling, recordkeeping, lending, remote storage and transfer to archival repository.

However, it is not only the archival regulations and the Archives Act that affect the recordkeeping functions. Several other laws and regulations must also be taken into account. This applies in particular to the *Freedom of Information Act* ("offentlighets-loven"), which has consequences for recordkeeping, presentation of public registry and screening of information. The *Public Administration Act* ("forvaltningsloven") provides general rules for the executive function, as well as more specialized provisions regarding professional secrecy and special access for parties involved (”partsoffentlighet”). The *Personal Data Registers Act* ("personregisterloven") and its regulation (”*personregister-forskriften”*) regulate the handling of personal information systematized as personal data registers. It is particularly worth paying attention to § 2-19 of the regulation, which regulates licensing and exemption from licensing for electronic records. The *safety instruction* ("sikkerhetsinstruksen") and *security and protection instruction* ("beskyttelses-instruksen") provide for the protection of information for reasons of state security or other reasons. Attention must also be paid to the written and unwritten rules known as «*god forvaltningsskikk*» [good administrative practice]. These include things like equality of treatment (precedent), the basis of decisions, allowing enough time for communication with public administrative bodies, etc.

It is not the task of Noark to implement the regulations in the recordkeeping function of public administration. However, the standard should support recordkeeping functions which are within the framework of the regulations, and it should avoid incorporating non-permissible functionality.

2.1.2 Record contents: record documents, case documents

According to the definition of the Archives Act, records are to be construed as documents which are produced as part of an activity ("dokument som vert til som lekk i ei verksemd"). This is a very wide definition which is in line with established custom in Norway and internationally. An organization's record documents are the documents that are received or produced as part of the activities of the organization. For posterity, they are the traces of the activities that took place, traces which document events in the form of decision, deals, information documents and other actions that have resulted in written information.

[4] Lov 4. desember 1992 Om arkiv.

An important consequence of this definition is that the concept of *record document* is not associated with any particular category of documents or to specific traditions in terms of case handling and records management. If a document has been produced or received as part of the organization's activity, then that document is a record document. Once entered into the records, a document stays there. The records should reflect the activities that are carried out. Thus, it is not permissible to remove certain documents, store them separately and claim that they do not belong in the records. In other words, the records are the central store of documents for the organization, including the executive function.

On grounds of space, retrieval possibilities, etc. -- i.e., the cost-effeciency of the recordkeeping function -- it is nevetheless necessary to limit the contents of the records to what is worth keeping from a documentational point of view. In Norway, this is regulated through rules of *records weeding*, and these rules will presumably be perpetuated through the regulations of the Archives Act. *Records weeding* filters out material which is not the subject of case handling, or material without documentation value for the organization, sometimes alluded to as "not of archival value". Examples of such material are duplicated (e.g., printed) material received from others, material downloaded from the Internet or external databases, draft documents and extra copies without documentation value, word processor files with draft copies of documents, etc. These normally constitute quite a large proportion of the material used or produced by executive officers. Records weeding is essentially carried out before the documents are entered into the records.

The records, then, consist of all material considered as record documents according to the Archives Act, except what is filtered out through records weeding. In addition to normal correspondence, notes, etc., the records also include an archival copy of own reports, circulars, etc., even if these per definition are duplicated and distributed. Also included are draft documents, etc., when valuable information important for the understanding of the case has been scribbled on them; in practice, this means the drafts which the organization finds it useful to preserve.

The Freedom of Information Act uses the concept of *case document* (or, more precisely, "case documents of public administration"). The case documents of public administration are, according to the Freedom of Information Act, either issued by an administrative body, or received by or presented to such a body. The concept of case document essentially corresponds to the concept of record documents for documents that are directly associated with the executive function. However, the concept of record document may have a wider meaning, since it includes registers, databases, etc., which would probably not be considered case documents.

The concept of case document is used in connection with records to designate those record documents that are directly associated with the executive function, and which are part of the *case records*. For all practical purposes, this must be regarded as equivalent to the same concept as used in the Freedom of Information Act. These concepts are expected to be used in the same way in the regulations to the Archives Act, reference being made to the provisions of the Freedom of Information Act.

Recordkeeping systems should be used to register and handle all documents that are part of the records, i.e., record documents and case documents as decribed above. Noark-4 has been designed to maintain these functions, and the boundaries between Noark and the SGK document storage are based on these principles, cfr. 2.2.2 below. In the rest of this report,

the concept of *document* is used in the sense of record document/case document unless otherwise specified.

2.1.3 Quality control in the recordkeeping function: involved parties and roles

Quality control in the recordkeeping function may be considered on two levels. On the one hand, the recordkeeping function itself is one of the foremost quality control functions of the organization. The following tasks are essential elements of quality control:

- The registry marks and registers all external inquiries and makes sure they are dealt with (stamping, filing plan code, entry into records, arrears control).
- The registry follows up all deadlines for external inquiries (maturity control) and the self-imposed deadlines of the organization (activation date, etc.).
- The registry documents both the pretext of the case handling (external inquiries), the decision-making process (internal documents and comments, drafts, etc.) and the results of the process (outgoing mail, decisions, deals, etc.).
- The registry provides for the systematics and coherence of the records, so that they can serve as a source and system of information for management and the executive function, and provide for legal and administrative documentation as well as knowledge and understanding for posterity (research, etc.).

On the other hand, it is necessary to consider the internal quality control of the record-keeping function, i.e., those mechanisms that are to make sure the recordkeeping function as such maintains the necessary level of quality. Important elements in this respect are the organization of the recordkeeping function, not least the distribution of rights and responsibilities. Normally, a number of parties are involved in the handling of case documents, and these perform various roles -- registrars, managers, executive officers, board secretaries, etc. In order to achieve a satisfactory level of quality in the record-keeping function, it is necessary to identify and define these roles, associate parties with the individual roles and assign to them tasks and responsibilities, rights and restictions of those rights. In this context, attention should be paid to the possibility that the roles may change with time, especially when electronic systems are implemented. An important element is granting the individual party the rights necessary to fulfil his or her role(s).

The recordkeeping function within public administration may be organized in many different ways. In large organizations, the tasks are normally specialized, and the individual party has only one or a few role(s). In small organizations, individuals will often have a wider spectrum of tasks assigned to them, and will thus perform several roles. The organization of the recordkeeping function itself may, for instance, consist of one single (or part of a) post, and one and the same individual may act as head of archives, executive officer and a board secretary. However, irrespective of size and organizational structure, it is important to have the roles defined, and to have decided what rights and responsibilities are associated with them.

Noark-4 is meant as a tool for maintaining quality control at both levels. The Noark systems should support the recordkeeping function in such a way that it fulfils its role as a quality control tool for the organization. In addition, Noark should have the necessary functionality to define roles and the corresponding rights, associate these with individual parties and check that these parties keep within the defined limits.

2.1.4 The position of Noark within the recordkeeping function

From the beginning, Noark has been rooted in the rekordkeeping of public administration. Essential information is registered about all case documents and and their processing, and this information is used in most parts of the recordkeeping function. It has gradually been deemed appropriate to extend the amount of information that is registered. This applies partly to information on cases and their associated documents, but in particular to various types of background information, such as an organization's filing plan, administrative structure, the names and addresses of clients, etc. Thus, the Noark systems now contain far more information than a traditional registry or diary system.

Noark-4 represents a big step forward in this development. The system provides for the registration of considerably more information than previously, both in terms of background information and information related to the individual cases or documents. The most significant enhancement, however, relates to the functionality of electronic recordkeeping. When case documents are stored electronically, even information such as notes, control information, etc., associated with those documents must be stored electronically. The result is a completely electronic recordkeeping system.

A completely electronic recordkeeping system according to the specifications of Noark-4 will achieve a dominant position in the recordkeeping function of an organization. It will contain most of the information that is used in connection with the recordkeeping function. It will be a management and information system for the records, and will also contain the records themselves. This will entail major changes both in the execution of the recordkeeping function and in the interaction with the executive function (see below).

Individual organizations may of course choose to give the Noark system a less dominant position than this (see 1.4 above regarding requirements at various levels). In its minimum version, Noark-4 may be used as a modernized version of Noark-3 and Koark. It is possible to limit oneself to registering records information and, if desired, decision-making information, and to keep the case documents including comments, control information, etc., on paper. Most organizations are expected to choose something between these two extremes in preparation for a gradual development towards electronic records.

2.2 How it relates to the executive function - SGK

2.2.1 Recordkeeping and the executive function

The recordkeeping and executive functions of public administration are closely related. The registry distributes documents to the executive function, follows up the processing with maturity and arrears control, receives and stores documents that have been processed, and makes information and documentation available to managers and executive officers. The interaction between the recordkeeping and executive functions are, in other words, extensive and of major importance to the efficiency of the organization.

Traditionally, this interaction has taken place by way of documents circulating in hardcopy form (on paper) and inquiries being made between the various institutions. For instance,

when an executive officer wants a document from the records, he or she inquires at the registry. The registry uses its information system to find the document, which is retrieved from the records and handed to the executive officer. This procedure is also to a large extent followed by organizations with Noark-based recordkeeping systems. The Noark systems themselves make it perfectly possible for the executive officer to search for cases and documents himself. However, since the recordkeeping system is not normally an integrated part of the tool that the executive officer uses, many find it too cumbersome (or don't have the knowledge) to use the recordkeeping system for searching themselves.

There is, undoubtedly, considerable potential for rationalization in incorporating as much as possible of the interaction between recordkeeping and the executive function into an electronic system, either by integrating the recordkeeping system in a complete case handling system or by integrating two or more systems with each other. If the desired potential is to be realized, the solution must include the following:

- It must be possible for all involved parties to reach the information they need and have access to, irrespective of where it resides in the system(s). Searching and retrieving must be possible within the user environment that each party normally uses, and with a user interface which does not vary significantly between the different parts of the system(s).
- It must be provided for electronic information and document flow between the different parts of the system(s) and between different parties, and for automatic updating.
- The recordkeeping must be electronic, so that the parties can retrieve documents on their computer screens.
- The roles and rights of the parties must be administered and managed by the system(s) in such a way that the individual parties only get access to the functions and information he or she is entitled to.

Noark-4 is designed with a view to being incorporated into such an integrated solution, both with general case handling systems according to the specifications of SGK and with the more specialized dedicated task systems.

2.2.2 Recordkeeping and the executive function in general: Noark and SGK

"Elektronisk saksbehandling. Statens generelle kravspesifikasjon (SGK)" [Electronic case handling. General specification of requirements for the state administration] was published by Statskonsult (the Directorate of Public Management) in 1997. Its purpose is to help public bodies evaluate various solutions and prepare their own specifications of requirements for electronic case handling. The specifications of SGK are primarily aimed at what is known as *general or non-standardized case handling*, i.e., various kinds of processing not associated with strictly defined handling procedures within a specific field. SGK is therefore relevant to most public bodies planning to implement an electronic case handling system. The specifications are mainly functional requirements at a general level. Thus, unlike Noark-4, SGK does not specify the information contents of the systems (apart from giving a few examples of document attributes) or data structure. Rather, the functional requirements are to be regarded as check lists for planning and designing case handling systems.

SGK is preoccupied with document handling, including document storage and retrieval. Executive officers should be able to handle both documents which are part of the (case) records and those which are not. Examples of the latter category are documents being drafted, either by an executive officer alone or in cooperation with others, documents which the executive officer receives or produces as member of external governing bodies, scanned versions of published documents, information downloaded from external databases, the Internet, etc. The executive officer should have access to various sources of information from one and the same user environment, and he (or she) should have access to flexible tools for organizing, associating and processing his documents. As part of this, he should be able to create his own folders where he stores "his" documents. An executive officer's folder might for instance contain one or more case documents (from the records) as well as other kinds of documents and information relevant to his handling of the case. Thus, SGK defines a separate document storage in addition to the case records of Noark, and documents in this document storage are managed by the individual executive officers. The document storage is subject to common rules in terms of document categories, a common registration form and common rules for deleting documents.

In the interaction between systems or functions based on Noark and SGK, respectively, it is essential to distinguish between the electronic (case) records of the organization, which are managed by Noark, and the document storage of SGK. The records are the documentation base of the organization. They are subject to comprehensive laws and regulations and strict requirements with regard to quality control. Documents in the SGK document storage are associated with the individual executive officers (or groups of officers) and managed by them. The document storage has a certain structure and certain rules for quality control, but it is up to the executive officers to enforce them in accordance with common guidelines. What documents the executive officers may want to include in their parts of the document storage will of course be depend on their needs. In many ways, the document storage is meant to replace the unstructured «file folders» in use and to give the officers an internal tool for working efficiently with documents during the production stage.

If documents belonging to the SGK document storage are stored in the records, the records will be loaded with documents which do not belong there (such as duplicated material, duplicates of record documents, documents being drafted, etc.) and which do not fulfil the quality control requirements for the records. It may be time-consuming to single out these documents at a later stage, such as during transfer to archival repository.

On the other hand, if case documents are stored in the SGK document storage instead of in the records, parts of the organization's documentation base will be taken out of its context and stored elsewhere without quality control requirements being maintained. If this should happen to a great extent, there is a risk that the archival authority (the National Archivist) would apply the same strict requirements to the SGK document storage as to the records, which would be very inappropriate and lead to inefficiency for all involved parts. Also, conflicts would arise with the Freedom of Information Act and, presumably, the Archives Regulation, if case documents were to be stored in the SGK document storage wihtout being registered in Noark.

Thus, the distinction between electronic records and the SGK document storage is fundamental in terms of laws and regulations and in terms of quality control. This imposes certain requirements in terms of the functionality of integrated systems, and in terms of the preparation and enforcement of procedures in the organizations that use the systems.

Technically, the distinction is mainly logical. Within one and the same system, both kinds of documents would be part of a common document storage. When an executive officer retrieves a document into his personal folder, this happens naturally through a reference to the record document, not by physical duplication. *From the Noark point of view, however, it is an absolute requirement that documents which are part of electronical records should be subject to the Noark functions for records management, including access control and quality control.*

Figure 2-1 presents a model for organizing document storage and retrieval in an interaction between Noark and SGK functions. The model is relevant whether the functions are integrated within the same system, or two or more systems are integrated with each other.

The model considers

- the needs of the individual parties (indicated by the roles of registrar, manager and executive officer) to have access to their documents and sources of information from one and the same user environment,
- the logical distinction between the case records and the SGK document storage, and the managing of the two parts by separate document-management systems,
- the need to transfer documents between the two documents storages, by way of actual document flow (in both directions) or by way of referencing (only from SGK to Noark).

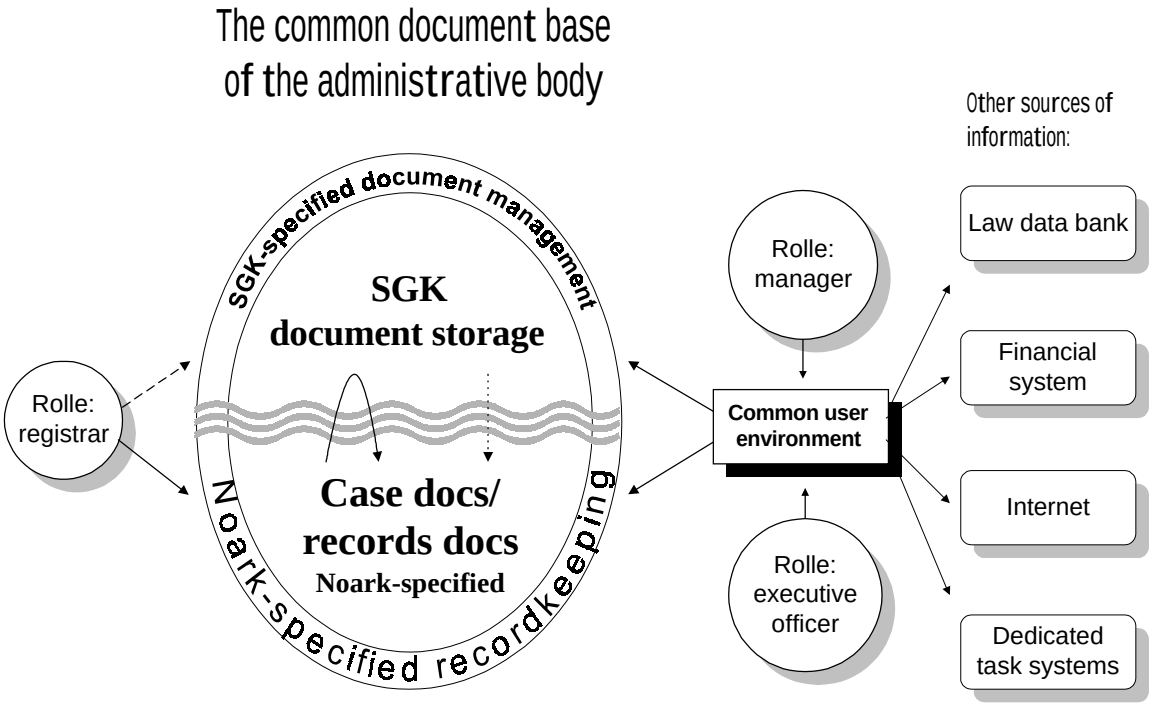


Figure 2-1: Model for document storage and retrieval in the interaction between Noark and SGK

Noark's interaction with the document handling of SGK-based case handling systems is particularly relevant during production of case documents which are to be stored as electronic records. The production of documents itself is an executive function outside the scope of Noark and within the scope of SGK, but the storage of documents as well as the associated registration and quality control are recorkeeping functions specified in Noark. This interaction imposes requirements in terms of the functionality of the systems as well as the firmness and clarity of procedures and responsibilities. This is described in more detail in chapter 6.

2.2.3 Recordkeeping and dedicated task systems

The need for integration between recordkeeping and case handling systems will also be present in those cases where the case handling system is a dedicated task system. Even here it is possible to choose between including the Noark functions in a complete system or integrating two or more systems with each other. The model in figure 2-1 applies even to dedicated task systems.

However, it will probably not be rational to build Noark functionality into every dedicated task system within public administration. There are a number of very different such systems, and it would take an unnecessary amount of development work to integrate Noark with all these. A more appropriate strategy is to integrate the dedicated task systems with the Noark interface, which would be common for "all" recordkeeping systems within public administration. Noark-4 forms the basis of such a solution by offering an open interface as specified in part II, chapter 17.

3. PRESENTATION OF NOARK-4

3.1 General description

3.1.1 Background and purpose

Noark-4 is based on previous Noark reports, primarily Noark-3 from 1994, as well as the Koark report of 1995. Noark-4 replaces these reports and now represents Noark standard, including Koark.

The purpose of Noark-4 is to specify requirements for as complete as possible an information and management system for the recordkeeping function of public administration. Systems which comply with these specifications, should be able to maintain the IT-based functions necessary for the daily recordkeeping, and should be able to store and retrieve the documentation -- documents and recorded information -- whose storage is the task of the registry. The systems should be so designed as to provide for the fulfilment of necessary requirements related to quality control in the recordkeeping function.

Noark-based recordkeeping systems should also work efficiently and flexibly in an integrated interaction with systems for general or specialized case handling as well as with systems for electronic mail and digital signatures. This presupposes that such systems use the communication interface which Noark-4 provides for and describes, or that the functions which Noark-4 describes are built into a more comprehensive system which also includes other types of functionality.

It should be possible to conserve the recorded information and documents stored in a Noark system for posterity. For this purpose, Noark-4 specifies how documents and recorded information should be exportable in a standardized format, on the one hand in order to establish internal historic databases, on the other with a view to transfer to archival repository. The export format should make long-term storage of the record material possible, including conversion into new platforms as technology changes. Standardized storage should also simplify long-term maintenance and searchability.

3.1.2 New functionality

Noark-4 represents the step from an electronic system for entry into records with a few additional functions to a completely electronic recordkeeping system. The change is considerable, partly because electronic records pose major requirements in terms of new functionality for the recordkeeping system, and partly because it provides for electronic communication and document flow as part of the work flow. New functionality directly associated with electronic records include the following:

- Case documents may be stored electronically in several versions and formats.
- The same case document may be associated with several cases and registry entries.

- Notes may be stored electronically and associated with case, registry entry or case documents in various versions and formats.
- Parties outside the registry (executive officers and managers) get extended access to registering in the records system, and the recordkeeping part of the decision-making process is managed by functions and status values in the system for entry into records.
- The system has functions for logging process information, etc.
- The recordkeeping system may be integrated with external e-mail, and provision is made for partly automated registering of e-mail received from other Noark-systems.
- The recordkeeping system may be integrated with or into a case handling system which includes electronic document flow, handling of documents and information residing outside the registry and electronic production of case documents.

There is also some new functionality which is not specifically related to electronic recordkeeping, such as:

- Several senders and/or addressees may be registered for the same document or registry entry (these functions are mentioned, but not specified, in Noark-3 and Koark).
- Individual follow-up of recepients is possible, in other words depreciation and arrears control.
- The association between inquiry and response is extended to include internal documents.
- The functional distinction between external and internal documents is abolished, but the document types are kept.
- The record structure is modified and made more flexible.
- The flexible record structure provides for differentiated principles of periodization and remote storage.
- Read access management is made clearer and firmer, and is more specifically associated with the provisions of the Freedom of Information Act.
- More differentiated write access management.
- Board-handling module of Koark is integrated in a slightly modified form.
- Some new reports such as statistical reports are specified, but the layout of information within the reports is left to the system developers to decide.

In spite of much new functionality, the basic structure of Noark remais unchanged. Case and document registration is carried out as before, and most of the information that is registered will be the same. However, no screen panels have been suggested in Noark-4. It has been left to the developers to design the panels and user interface as they select technical solutions.

3.1.3 Requirements for procedures and ways of working

The specification of requirements discusses the design of the recordkeeping system, not the use of it. Still, there will always be a connection between the design of the system and the user procedures and ways of working. The specification of requirements is based on a given set of recordkeeping and decision-making procedures, and the systems which become commercially available will influence and to a wide extent determine the ways of working and procedures of public administration. Within this framework, however, there is

usually ample scope for flexibility in the detailed drawing up of procedures. The systems, as specified in Noark-4, offer many opportunities for choice in terms of practical application, and user organizations may choose whether or not to implement a number of the functions.

The most significant change in terms of ways of working occurs when electronic record-keeping is implemented, possibly in combination with an electronic case handling system. Such a transition is bound to influence the distribution of roles within the organization and the interaction between the various involved parties, and it will change people's tasks and the sequence of these tasks. The implementation should be carefully planned. It must be decided whether to implement in one operation or gradually. A gradual implementation will involve a combination of paper-based and electronic recordkeeping, and it must be decided what kind of combination can be handled in an appropriate way. Adequate tools and procedures must be provided for, so that electronic record material may be preserved in the long term and through technological changes, possibly until an external archival repository is ready to take over responsibility. Noark-4 offers no complete guidelines as to the implementation of electronic recordkeeping, but chapter 5.5 draws attention to a number of details which should be considered at the planning stage.

It should be noted that Noark-4 has no intention or authority to *impose* particular procedures on users. Such injunctions must be justified by current laws and regulations. The intention of Noark is to provide for good procedures within the existing regulations at the time of publication of this report. There may, however, be cases where opportunities described in Noark are restricted by adopted regulations. For instance, the National Archivist might restrict opportunities for periodization of records as described in chapter 12. In such cases, the laws and regulations do of course take preceedence of any possibilities described in Noark.

3.1.4 Gradual implementation of new functions and procedures

The new functionality of Noark-4, and its associated procedures, may be impemented gradually. Suppliers who develop systems according to Noark-4, may choose to start with the basic functions (see ch. 1.4) and extend the system gradually, or they may choose to offer versions at different levels, for instance with or without electronic recordkeeping. Administrative bodies will be able to choose to what extent they want to implement new functionality. Some of them will probably choose to use paper-based recordkeeping for the foreseeable future, while others are gradually preparing for the implementation of electronic recordkeeping.

Thus, in the years to come, Noark-based systems and the usage of public administration are likely to be spread across various levels. What is common to all, is the fact that the basic functions comply with the Noark-4 specifications, and those who go beyond the basic level, will also follow a common set of functionality and procedures complying with the enhanced specifications. This way, both systems and procedures may -- should the wish and need arise -- develop towards the higher levels of Noark-4, including integration with e-mail and electronic case handling. Noark-4 is intended to include functionality with an adequate potential for development for years ahead.

3.2 Main structure of Noark-4

Noark-4 is described in terms of five modules. In this context, "modules" is not to be perceived as independent system modules which may be combined according to need. Each module describes a main function, closely integrated with the rest, and it cannot function independently of these (except one of the modules). Together, they offer a total solution for electronic registering, storage and retrieval of document-related information and documents.

The five modules are:

- Module for registration and records management (records management module)
- Module for electronic recordkeeping
- Module for administrative structure and record structure (record structure model)
- Module for access control and user management (access-control module)
- Module for board handling (board-handling module)

Three of the modules are compulsory if systems are to comply with Noark-4. The module for electronic recordkeeping and the board-handling module may be omitted, but if included, they must follow the specifications. Electronic recordkeeping represents the top level of the specifications, and needs to be included only in the the most advanced systems. The board-handling module is a necessary part of systems delivered to the local administration sector, and it may be of interest even to state bodies where advisory and governing boards take part in the decision-making process.

The m*odule for registration and records management*, hereafter referred to as the *records management module*, is the core of a Noark system. This is where all incoming and outgoing case documents are registered, going to or from external clients or internal units. The documents are associated with cases. The cases are associated with folders (through file code) and records, as well as with executive officer and administrative unit. The module also maintains the usual follow-up functions, including checking up on deadlines for processing, depreciation and arrears control, etc. It also makes it possible to register internal notes for cases and documents, capture and store processing logs, etc.

The concept of *records management* is introduced as from Noark-4. It is meant to indicate that this is where the recordkeeping functions of an organization are managed. This keeps track of case documents, be they electronic or on paper, as well as all information associated with those documents. Access to electronic case documents is managed through this module. In Noark-3 and Koark, the corresponding functions are referred to as the *registry system* ("journalsystemet") or *registry section* ("journaldelen"). However, the records management functions go so far beyond traditional recordkeeping that a change of concept was deemed appropriate.

The *module for electronic recordkeeping* is that part of the system which stores the documents (case documents, etc.) in electronic form. The documents are mainly accessed through document registration *(registry entry)* in the records management module, but certain kinds of documents (such as minutes) are accessed from the board-handling module. One and the same electronic document may have several *functions* (e.g., be a main document or an attachment), and it may be stored in several *versions* and several *formats*. Thus, the relationship between registry entries and electronically stored documents may vary a great deal.

The *module for administrative structure and record structure,* hereafter referred to as the *record structure module, is a support module* for the records management system. Noark-4 provides for the registration of an arbitrary number of levels within the organization's administrative structure. The record structure distinguishes between record-organizational units *(registry management units)* on the one hand and physical/logical units for storage of record documents (*records* and *record sections*) on the other. By splitting records into records sections, which are freely defined parts of records, it is possible to establish more flexible and controllable solutions for periodization and remote storage of record material, implementation of new filing plan, etc. Records sections may also be used to define record series with their own organizational principles (e.g., object series and board documents).

The m*odule for access control and user management,* hereafter referred to as the *access-control module,* manages and controls all use of the system. The individual user is assigned one or more *roles,* and based on this the system decides what functions the user has access to. Access to information within the system, i.e., read access, is controlled by the individual user's administrative and/or record-organizational association and by *access codes,* which are tagged onto information to be screened. It is also possible to define *access groups* with access to specific information and documents according to need.

The *module for board handling,* hereafter referred to as the *board-handling module,* is a tool for managing the work flow of collegiate bodies such as boards, councils, committees, etc., and storing documents from this process. The module is specifically designed to manage the work flow of local and regional political bodies, but is presumably of interest for others with similar decision-making procedures. The board-handling module includes processing plan and processing history for individual cases, association with recorded case documents, preparation of case plans for meetings, production and storage of board-related documents (such as summons to meetings and minutes), etc.

The formalized main structure of Noark-4 shows the relationship between the individual modules. The individual modules are described in more detail in chapters 4 - 5 and 7 - 9.

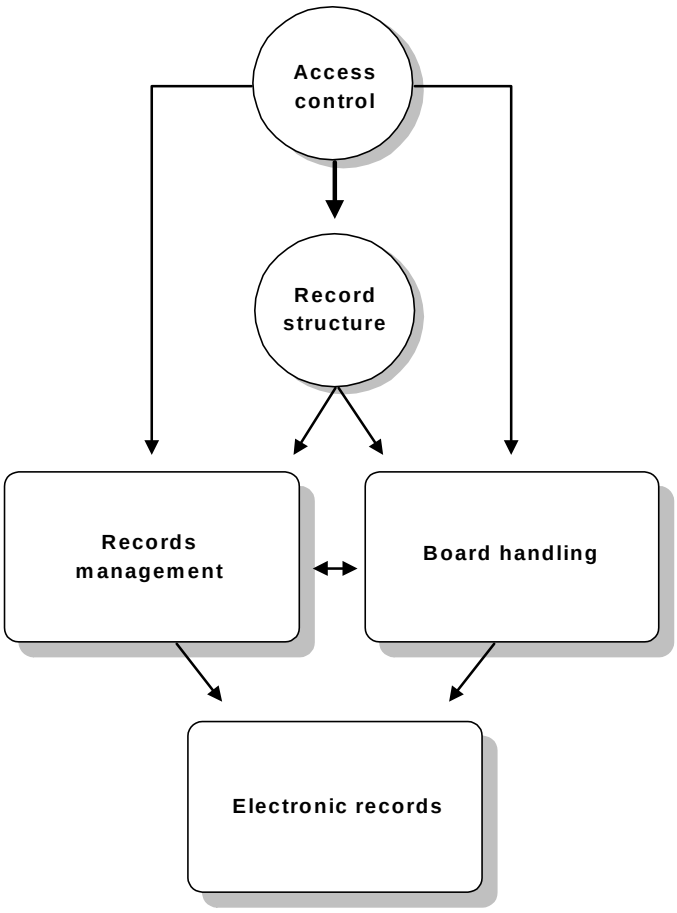


Figure 3-1: Main structure of Noark-4

Modules shown as circles are auxiliary modules, which means they contain functionality which is not of primary importance to a recordkeeping solution, while still providing important functionality for supporting the use of it. The functionality of the auxiliary modules are, however, an obligatory part of Noark-4-compliant solutions. The rectangular boxes represent the "operational" modules, the only obligatory one being the records management module.

3.3 Main functional requirements

The following functional requirements apply in general for Noark-4:

3.3.1 User interface

K3.1	The user interface of all modules should be based on common principles, so that the user threshold is as low as possible. All panels, dialogues, etc., should give a uniform impression. The same term should be used when a function is repeated in several parts of the system.	A

K3.2	All text and messages should be in Norwegian.	O
K3.3	It should be possible to choose between "bokmål" and "nynorsk" for messages and text.	A
K3.4	There should be help for all the functions that are available to the user.	O
K3.5	There should be help for each field, function, pushbutton, etc.	A
K3.6	The user should be given informative messages in any error situation. In cases where giving adequate information in the message is not possible, it should be indicated where further information may be obtained.	O
K3.7	The individual user's access to information should be limited by his/her role(s) and the access control of the system, as discussed in chapter 8.	O
K3.8	The included modules should be closely integrated so that they are perceived of as a system by the user. This means that all information which is necessary for a specific task, should be immediately accessible, irrespective of what module the information belongs to.	O
K3.9	For tables between which relationships have been defined, such as Case - Registry entry, Cfr. case - Case and registry entry, Registry entry - Sender/addressee, it should be possible to open the relationship. It should for instance be possible to view all registry entrys associated with a case. This does not apply to help indices.	A

3.3.2 Registration functions

K3.10	The registration panels should be designed so as to make the registration as efficient as possible. If possible, all fields used in connection with a task, such as the registration of an incoming document, should be accessible in the same panel.	A
K3.11	It should be possible for the individual user to decide the sequence of the runthrough of attributes (fields) in the panels during registration. It should be possible to skip attributes which are used infrequently, while at the same time having easy access to those attributes if desirable.	A
K3.12	It should be possible to store and retrieve the aforementioned registrations sequences (see previous point).	A
K3.13	All information that is registered or changed, should be immediately accessible to other functions and other users (within the limitations posed by the rights of the individual user, cfr. ch. 8).	O
K3.14	It should not be possible to make registrations or changes that conflict with the principles of the technical description.	O
K3.10	For fields where the table description specifies lookup in a help index, it should be possible to retrieve a summary of permissible values from the help index, based on the criteria specified in the technical description.	O
K3.11	For help indices (see previous requirement) where the number of	A

	values may be high, it should be possible for the user to search for the correct value based on information in the help index and, where appropriate, other tables associated with it.	
K3.12	For fields for which the table description specifies lookup in a help index, it should not be possible to register values which do not exist in the help index, unless the technical description specifies explisitely that this is permitted.	O
K3.13	During registration of new records, the system should, where possible, display the fields in the registration panel already filled in with default values based on the context in which the registration is carried out and on the role of the user. As a minimum, the default values described under the individual attributes should be used.	O
K3.14	The presentation of dates in panels should be configurable. If not configurable, the format should be DDMMYY (day, month, year).	A
K3.15	All dates/times should be stored using 4 digits for years. The same applies to years which are part of a case number, serial number, etc., irrespective of whether two or four digits are displayed in the panel.	O

3.3.3 Searching

K3.21	All attributes with a length restriction (i.e., not free-text fields or binary fields) in all tables should be searchable.	O
K3.22	Information described as derived attributes in chapter 14 should be searchable, just like any other attribute.	O
K3.23	It should be possible to make any search case-insensitive.	O
K3.24	In a search, it should be possible to specify values for several fields in the same table using an AND operator between the fields.	O
K3.25	In a search, it should be possible to specify an OR operator between fields or groups of fields.	A
K3.26	For all date fields and numerical fields, it should be possible to search for intervals of values.	O
K3.27	For text fields with length restrictions, it should be possible to use left or right truncation while searching.	O
K3.28	For text fields with length restrictions, it should be possible to mask single characters while searching.	A
K3.29	Free-text searching (i.e., searching for any word in a field) should be available in all text fields, whether they have length restrictions or not.	A
K3.30	Where appropriate, it should be possible to search for information from several tables similtaneously. This applies in particular to the tables *Case, Filing plan code, Part in case, Registry entry, Sender/addressee* and *Document description*.	O1
K3.31	It should be possible to do further searches beyond the records found in the previous search by adding new criteria to the existing ones.	A

K3.32	Users should be informed of the number of hits for a search.	O
K3.33	The system should have functions which prevent the user from inadvertantly starting a time-consuming search.	A
K3.34	The system should provide information on the estimated time required to perform a search.	A
K3.35	It should be possible to cancel a search in progress.	A
K3.36	The individual user should be able to choose if the result should be displayed only in terms of the number of hits or as a list with selected attributes from the records found.	A
K3.37	The individual user should be able to decide which fields should be displayed in the result list for a search (see previous point).	A
K3.38	It should be possible to store and retrieve the setup (layout) of result lists (see previous point) as needed.	A
K3.39	The individual user should be able to choose the sorting principle for the results of a search.	A
K3.40	It should be possible to get printouts based on the results of a search.	A
K3.41	It should be possible to store and retrieve a set of search criteria (predefined search) as needed. It should be possible for the user to change search criteria retrieved this way before the search is carried out.	A
K3.42	Any search should be restricted according to the access provided by the user's roles, authorization for access codes and membership of access groups. This means, for instance, that if the user searches using a criterion for one specific attribute, then the search should not produce hits for records where the user is not authorized to view this attribute, even if other attributes of that record are accessible.	O

3.3.4 Technical design

K3.43	The system should handle the transition to year 2000 without requiring any user input.	O
K3.44	The system must be adapted for use with standard backup solutions. Descriptions of backup procedures should be included in the system documentation.	O
K3.45	The system must have recovery functions, so that the integrity of information is maintained in case of interruption due to power failure or computer breakdown.	O
K3.46	It should not be possible to delete records that are referenced from other tables.	O
K3.47	It should not be possible to change key attributes used for referencing from records in other tables without changing the corresponding attributes in the referring records.	O

K3.48	All functions which involve updating more than one record, should be performed in such a way that all or none of the records are updated.	O
K3.49	The system should be secured so that noone gets access to information for which they are not authorized, if they try to use other tools than the Noark system.	O

3.3.5 Additional information

If the system provides for adding information beyond the requirements of Noark-4, this information must be regarded as record material like the rest of the Noark base. This means that all such information should be exportable according to the principles of chapters 14 and 15 (see also K12.12).

A Noark system that satisfies the basic requirements of Noark-4, cannot be enhanced with additional information representing alternative solutions to the specifications of Noark-4 at a higher level.

K3.50	If the system includes attributes which are not specified in Noark-4, these should be exportable as additional information according to the principles described in the table *Additional information* (14.2.31).	O
K3.51	A Noark system should not be able to substitute for the attributes defined in Noark-4, correponding or similar data elements under other names or with another structure, etc. If the system uses other attribute names internally than those specified in chapter 14, these must during export be converted to the names specified by Noark-4 (see chapter 15).	O

3.3.6 Simplicity

Noark-4 specifies a rather complex functionality in many areas. This is necessary in order to offer the advanced solutions demanded by a number of administrative bodies. On the other hand, many organizations obviously have very limited need for the more complex functions. The most common tasks usually involve simple functions, and it is important that these can be carried out in a simple and rational way. Simple tasks should be simple to perform. Simple and frequently used work operations should not be weighted down by the system's offering more advanced functionality within the same area. The following are examples of such operations:

- Noark-4 allows for the registration of several senders and addressees for one and the same document (see chapter 4). Nevertheless, there should be a simple and rational way of registering the most frequent combinations:
  - one sender on an incoming letter
  - one addressee on an outgoing letter
  - one sender and, optionally, one addressee on an internal document
- A registry entry may be associated with several electronic documents in several versions, and, similarly, a case document may be associated with several registry entries, cfr. chapter 5. There should nevertheless be a simple and rational way of

associating one document in one version and one format (i.e., one copy) with one registry entry.

- A Noark base may include several record entities which may in turn contain several records sections (see chapter 7). Still, there should be a simple and rational way of using a base which only includes one records entity consisting of only one records section.

It is impossible to formalize requirements of this kind, since it is not possible to decide whether the requirements are satisfied or not. The requirement concerning simplicity is therefore only a general appeal to system developers. The user-friendliness of the system will to a wide extent depend on the degree to which this reqirement is met.

4. MODULE FOR REGISTRATION AND RECORDS MANAGEMENT

4.1 Purpose of module

The module for registration and records management («records management module») covers a number of functions, of which the most important are:

- registrating, storing and retrieving information on case documents and attachments (registry information, etc.)
- linking case documents to cases
- managing access to information on cases and documents, as well as access to documents which are stored electronically
- linking cases and associated documents with the record structure and physical records of the organization
- providing an overview of basic work-flow elements:
- administrative basis, case-responsible, executive officer
- processing deadlines
- depreciation status (cfr. arrears control)

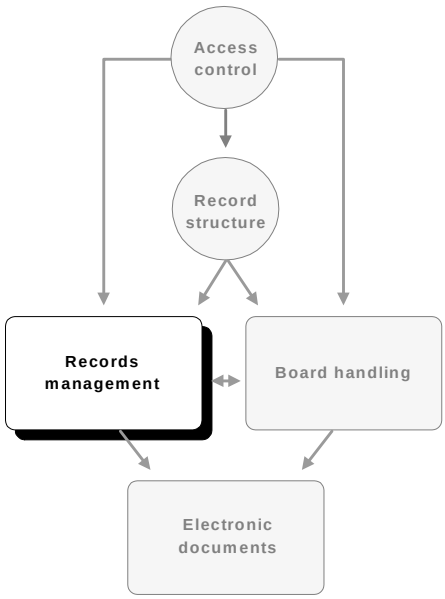


Figure 4-1 Position of records management module in Noark.

- registering, storing and retrieving notes, activity logs, etc., associated with the decision-making process
- producing reports in connection with the recordkeeping functions of the organization, including:
- registry printouts (public registry, etc.)
- lists of senders/addressees
- arrears lists
- processing statistics

The requirements with regard to the design of the records management module are given in this chapter, except the requirements regarding reports, which are treated in separate chapter together with the other reports in the Noark system (ch. 11).

4.2 Module design

The essential tables of the records management module are *Case* and *Registry entry*. In *Case*, new cases are created and information on individual cases registered, i.e.,

information which is common to the documents of the case (cfr. 4.2.1 on the concept of *case*). In *Registry entry*, information on individual documents is registered. A case includes one or more registry entries, and a registry entry is always associated with one case. The relationship between *Case* and *Registry entry* is, in other words, one to many (1:M), and for a new registry entry to be created, there must always be a case to associate it with.

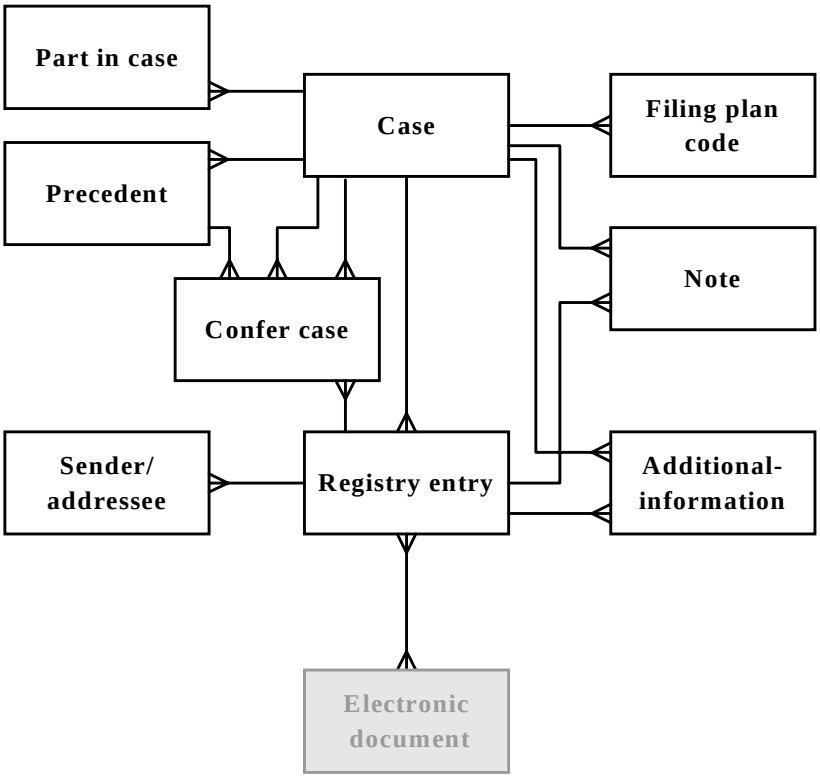


Figure 4-2: Simplified data model for records management module (see chapter 14 for complete overview)

The *Registry entry* table corresponds to *Document* in Noark-3 and Koark (compare also the concepts of "document register", "document level", "document information", etc.), and it thus contains information on the case documents. The name of the table has been changed because Noark-4 also specifies electronic storage of the documents themselves (case documents and other documents), and the concept of *document* must be reserved for these. Note also that some of the information in the document register of Noark-3 is taken out of the transaction-record table of Noark-4 and inserted in separate tables.

The following general functional requirements apply to the records management module:

K4.1	It should be possible to register a document received or produced by an organization in a registry entry. As a minimum, it should be possible to register information which is obligatory in the table *Registry entry* (see chapter 14).	O
K4.2	When created, a registry entry should always be associated with a case. One or more registry entries may be associated with a case.	O
K4.3	As common information on a case, it should as a minimum be possible to register the information which is obligatory in the table *Case* (see chapter 14).	O
K4.4	It should appear from the relevant panels that information is registered on two levels: one for the case and one for the associated registry entry. It should be possible to register on both levels in one operation.	O
K4.5	It should appear from the relevant panels how many registry entries exist for a case, and it should be possible to move between these records and view the contents of a specific record.	O

4.2.1 The concept of case

The relationship between *Case* and *Registry entry* must be considered in view of the concept of case, which has always been essential in the Noark standard. The concept of *case* is based on a similar use of the concept in the Public Administration Act and the Freedom of Information Act. None of these acts defines the concept; they use it in an abstract way, partly to denote a *case that is being dealt with or processed* (based on an external inquiry or internal initiative), partly about the *processing itself*. In a concrete sense, it applies to the case documents, registrations, notes, etc., which arise during and/or are part of the processing.

In Noark, a case is something concrete, consisting of one or more registry entries and their associated documents linked together under a common identity. The documents of a case deal with a matter that is being processed, and they represent (or "constitute") the processing of this matter.

It may occasionally be difficult to decide what is a matter for processing, and thus which documents belong to one case. There is no universally valid definition for this, but it is usually quite easy to decide. If, for instance, there is an inquiry which is to lead to a decision through a decision process, it is usually appropriate to define this as one case. The most common example of this is a case which only requires a simple answer. However, there may also be comprehensive and complex cases of this kind, e.g., employment cases, licensing cases (applications for licenses) or construction cases (applications for construction licence).

It must be stressed that the case concept of Noark is not primarily a question of what is correct and what is incorrect, but rather of how it can be used in an appropriate way. Registering cases and case information is primarily a tool for grouping case documents which belong together, under a common identity, which facilitates clarity and retrieval for both electronic records and physical records. The use of a separate case level replaces the traditional linking that was used with manual registration.

In Noark-4, it is also possible to associate cases with each other in a higher-level group *(project)*, and to establish sub-groups of registry entries (documents) within a case *(division of cases)*. This is described in more detail in paragrapgh 4.2.3.

4.2.2 Identifying case and registry entry

The identification of cases and registry entries is among the most fundamental elements in a Noark system. The following requirements apply:

K4.6	*A case* is identified through its *case number*. The case number consists of a year (see the attribute C*ase year*) followed by a serial number (sequence number of case) within that year (cfr. the attribute *Sequence number of case*).	O
K4.7	The case number should be displayed to the user as yy/######, where yy are the two last digits of the year and ###### is the sequence number, displayed with up to six digits, but omitting preceeding zeros.	A
K4.8	It should not be possible to delete a registered case or to modify a case number.	O
K4.9	A *registry entry* is uniquely identified through its *serial number*. The serial number consists of the year (cfr. the attribute *Record year*) and a sequence number within that year (the attribute *Sequence number of registry entry*).	O

The serial number is primarily an internal identification number for the system, but it may also be useful to the user, especially in a presentation of chronological document lists, be they on screen or in a paper printout.

K4.10	The serial number should be displayed to the user as #######/yy, where yy are the last two digits of the year and ####### is the sequence number, displayed as up to seven digits, but omitting preceeding zeros.	A
K4.11	It should not be possible to delete a registered registry entry or to modify its serial number (which is the internal identification of the system).	O
K4.12	It should also be possible to identify a registry entry through its *document number*, which is a serial number within the individual case (4 digits).	O

The document number is the main number for the users' identification of a registry entry. Complete identification of a registry entry involves a combination of case and document number (usually called "case and doc number").

K4.13	Case and document number should be displayed as yy/######-dddd, where yy/###### is the case number as specified above and dddd is the document number of the registry entry within the case, displayed as up to four digits, but omitting preceeding zeros.	A

The case and doc number of a registry entry may be modified if a case is split up and/or records moved to another case. This is discussed in more detail in paragraph 4.2.4.

4.2.3 References and main structures in terms of case and registry entry

Individual *cases* are linked to the record structure of an organization through references to *registry management unit* and *records section*, as well as through *coding according to filing plan.* The latter involves assigning one or more *order values* or *filing plan codes* (subject codes and/or object codes) to a case document. The coding links together cases which belong together thematically. In paper-based recordkeeping, the filing plan code is also the address of the folder where the case is stored physically. The record structure is described in chapter 7.

K4.14	When a case is created, the attributes *Registry management unit* and *Records section* should be filled in automatically. The values are obtained from the roles the assigned to the user, cfr. the table *Person/Role*. The user should be able to change the values.	O
K4.15	In the basic version of Noark-4, it should, as a minimum, be possible to classify individual cases using two order values (file codes). The file codes should be subject codes and/or object codes, and it should be possible to rank them as primary and secondary codes. The organization should be able to choose filing plan code according to the standard key of the state administration (and other keys which follow the same principles) as well as the municipal K-code system.	O
K4.16	In the enhanced version of Noark-4, it should be possible to classify a case with an arbitrary number of order values (file codes) – subject codes and/or object codes. It should be possible to rank the file codes (primary, secondary, tertiary, etc.), but it should also be possible to register file codes without rank. They will then function as references to other subjects or objects to which the case belongs.	O1

A case is assigned administrative basis for processing through references to *Case-responsible unit* and *Case-responsible (person).* The layout of the administrative structure belongs to the record-structure module and is described inchapter 7.

K4.17	It should be possible to associate a case with the administrative structure of an organization by filling in the attributes *Case-responsible unit* and *Case-responsible* (person - initials). The system should only allow values which have have already been registered in the system - see chapter 8. If the initials of the person responsible for the case are unique across administrative units, then *Case-responsible unit* should be filled in automatically as the initials of the person responsible for the case are registered.	O

Several cases may be grouped together in a *project.* A project is thus on a higher logical level than a case, but the project is only a shared category belonging to the cases, and it is used when it is appropriate to group together cases with something in common, such as an actual project. By searching for projects, it is possible to retrieve the cases which the project consists of.

K4.18	It should be possible to group together cases in a *project.* A project is a shared category which may be used to search for cases which are	O

	grouped together.	

A case may also refer to one or more other cases, or to documents within cases, without being defined as belonging to a project. Such references are likely to be used in situations where a case contains information which is relevant to one or more other cases, as a kind of cross-reference. (See also chapter 4.6 on changes in the cross-reference field as compared to Noark-3 and Koark).

K4.19	In the basic version, it should be possible to refer from one case to another.	O
K4.20	In the enhanced version, it should be possible to register references from one case to one or more other cases, and to one or more individual documents (registry entries) within a case. The table *Confer case* is used for this purpose.	O1

A *registry entry* is directly linked to a case and thereby the record structure, administrative basis and, possibly, a project and other cases. In Noark-4, functions are specified for grouping registry entries in several sub-groups *(case sections)* within a case. Such *division of cases* is primarily adapted for categorization of various types of documents within a case, which may, for instance, be used to specify groups of documents which shed light on different aspects of the case. Case sections may also in some situations be stored separately - see below concerning procedures. It must, however, be pointed out that the division of cases does not directly concern the referencing from registry entry to case, nor the numbering in the form of case and document number. Division of cases is further described in chapter 7 concerning record structure.

4.2.4 Splitting up and combining cases; moving documents

Noark-4 specifies functionality for splitting a case into several cases, and for combining several cases in one. In practice, this means that one or more registry entries are moved from one case to another, possibly after one or more new cases have been created.

The need to *split up* a case may arise as a consequence of erroneous registrations (a document may, for instance, be registered as a new document in the wrong case) or because the case develops in several directions. The split is is effectuated by removing one or more registry entries from the case in question and associating it/them with another case (possibly after creating a new case). Technically, the move is carried out by changing the case number for the registry entries in question and giving them new serial numbers (chronological, in ascending order) within the new case. Registry entries which remain with the old case, may keep their existing serial numbers, or renumbering may be carried out. If the existing document numbers are kept, the system must be able to handle holes in the document-number sequence within a case.

The need to *combine* several cases in one may arise as a consequence of erroneous registrations (for instance, a new case is created for a document which belongs to an existing case) or because one takes a different view of the case in question after some time. The combination is effectuated by moving all registry entries from one case to another, which means, technically, that the case number of those records is changed. Thus, the case from which the records are moved, loses all its registry entries and ceases to exist.

However, as said before, the case itself cannot be deleted. The system must be able to handle "empty" case numbers. In the case to which registry entries are moved, it should be possible to choose whether to sort all records chronologically (in ascending order of serial number) and assign new document numbers, or if the records that result from the combination action should come after the old ones.

Splitting up and combining cases require resources, accuracy and checking (see ch. 4.3 on procedures). For this reason, it is recommended that this be carried out only where strictly necessary for the expedient use of the system. Note also that the possibility of dividing cases (see 4.2.3 above) may in some situations be an alternative to splitting them up.

K4.21	It should be possible to move one or more registry entries from one case to another. This move involves assigning a new case number to the record(s). The case numbers must not be changed.	O
K4.22	Registry entries which are moved, should automatically be assigned new document numbers starting with the first available number in the case to which they are moved. New document numbers are assigned in ascending order according to the sequence (document numbers) the registry entries had in the case from which they were moved.	O
K4.23	Registry entries which are *not* moved, should not have their document numbers changed, unless renumbering is carried out for the records within a case (see K4.24).	O
K4.24	It should be possible to move all registry entries which are associated with one case section, in one operation.	A
K4.25	It should be possible to renumber the document numbers for all registry entries within a case. Renumbering should always include all registry entries within a case and be effectuated in one operation. The sequence should follow the ascending serial numbers of the records.	O
K4.26	If moving and/or renumbering affects references to or from the registry entries concerned (e.g., for depreciation - see paragraph 4.2.7 - or for references as described in paragraph 4.2.3), the references should be updated automatically, so that the system is consistent after moving/renumbering.	O
K4.27	The system should not allow the moving of a registry entry which depreciates or is depreciated by other records which are not moved - see depreciation linking, paragraph 4.2.7. If this is attempted, the user should receive a message informing him of which links are blocking the move operation.	O
K4.28	All moving and renumbering should be carried out using a special set of commands, and only by authorized personnel according to the rights defined in chapter 8. All moving and renumbering should be logged by the system in a clear way.	O
K4.29	During moving and renumbering, the user should be reminded to change references as necessary on paper documents in the records.	O

4.2.5 Document types

Registry entries in Noark are associated with different document types, which indicate the kind of function that the registered documents have. Permissible values for *document type* in a registry entry are specified in the table *Document type* and include the following:

I Incoming letters
U Outgoing letters
N Internal documents (memos, reports, etc.) which require following-up and depreciation in the registry
X Internal documents which do not require following-up or depreciation
S Case drafts and other registered documents associated with the decision-making process (minute, opinion).

Note that "internal documents" in Noark means documents which are communicated internally within a unit, or between units which register in the same Noark base, hence base-internal documents. This does not always correspond to the concept of internal documents in the sense of the Freedom of Information Act - see paragraph 7.3.2.

K4.30	Document types are registered in the attribute *Document type* in the registry entry. The system should only allow the values which are specified in the table *Document type*.	O

4.2.6 Sender and addressee; parts in a case

Noark-4 four has moved some essential registration information, such as *registry management unit, executive officer* and attributes for *depreciation*, from the registry entry itself to a separate table for S*ender/addressee*. This makes it possible to register several (senders and) addressees on one and the same document, and to follow up the processing separately among the individual addressees. In the basic version of Noark-4, it is still possible to let the system restrict the number of senders and addressees to one, for instance by keeping these attributes in the registry entry.

The following functionality is assumed with regard to the registration of sender and addressee for the individual document types:

K4.31	In the basic version, it should as a *minimum* be possible to register • for document type I: one sender (must be filled in) • for document type U: one addressee (must be filled in) • for document types N, X and S: one sender (must be filled in) and one addressee (must be filled in for document type N).	O
K4.32	In the enhanced version, it should be possible to register the *sender* as follows: • Document type I: it should be possible to register one or more senders (one is obligatory). It should be possible to register all but one as co-senders. • Document types U, N, X, S: there should always be only one (responsible) sender. In addition, it should be possible to register co-senders. • Specifically for document type U: the default value for sender	O1

	should be the organization itself; this should be registered automatically by the system. It should be possible to change the value.	
K4.33	In the enhanced version, it should be possible to register *addressee* as follows: • Document type I: there should always be only one (responsible) addresse. The default value should be the organization itself; this should be registered automatically by the system. It should still be possible to change the value. In addition, it should be possible to register CC addressees. • Document types U, N, X, S: it should be possible to register one or more addressees (one is obligatory for document types U and N). It should be possible to register all addressees except one as CC addressee.	O1
K4.34	For all internal senders and addressees, it should be possible to register administrative unit and executive officer (initials). The system should only allow values which have already been registered in the system - see chapter 8.	O
K4.35	If the initials of the executive officer are unique across administrative units, then the administrative unit should be filled in automatically as the initials of the executive officer are registered.	A
K4.36	It should be possible to have help indices with names and addresses of clients (address registers), and it should be possible to use these for looking-up during registration of senders, addressees and parts in a case. It should be possible to refer to the individual entries in the address register by way of short names. When the short name for a sender or addressee is registered, the system should automatically retrieve information from the address register to the registry entry (or the sender/addressee table).	O
K4.37	It should be possible to group clients in the address register and refer to such address groups through an abbreviated name and/or common identifier. It should be possible to register address groups together as addressees (or as senders) on a document. In summary panels, the system should be able to display the common identifier and the number of senders/addressees the group consists of. There should be functions for toggling between the common identifier and detailed information on individual senders/addressees.	O1

It should be possible to register persons and organizations who are parts in a case, in Noark to ensure, for instance, that they get sent documents they are entitled to in connection with the procesing.

K4.38	It should be possible to register one or more parts in a case (see the table *Part in case*.	O1
K4.39	It should be possible to enter in one operation parts in a case as addressees associated with a registry entry in the case.	O1

4.2.7 Functions for depreciation and completion of cases

Registry entries containing document type I or N are subjected to arrears control and must be depreciated in order to be kept outside the arrears list. According to the technical specification of Noark-4, the depreciation attributes no longer reside in the transaction-record table itself, but in the subordinate sender/addressee table. Separate depreciation may be effectuated for each addressee, which is particularly relevant for document type N. Depreciation is carried out in the following two ways:

- Direct depreciation: the user registers *mode of depreciation* (e.g., "T.E.", i.e., ”for notification”), and *depreciation date* is filled in automatically by the system.
- Automatic depreciation: during registration of reply document, the user specifies document number for the document(s) which is/are replied to (cfr. the attribute *Replies to document*). The system links the reply document to the document(s) replied to. When the registry status of the document is set to J (registered in the records) - see chapter 6 - the system automatically carries out depreciation of the document(s) replied to. The reply document must, of course, be registered in the same case as the document(s) replied to.

K4.40	It should be possible to depreciate a received document of document type I or N in the registry by registering *mode of depreciation*. This indicates that the document has been processed by the addressee. The system should automatically set *depreciation date* to the current date, but it should be possible to change this date.	O
K4.41	It should also be possible to depreciate one or more received documents of document type I or N by registering a reply document. The reply document must be registered in the same case as the documents for depreciation. The reply document is associated with the received document(s) through registration of the document number of the latter. This should have the following effects: • The attribute *Replies to document* on the reply document is filled in automatically with reference to the received document. The reference should be displayed as document number in the relevant panels. If more than one document is replied to, the reference is set to 0. • The attribute *Depreciated by document* on the received document(s) should be filled in automatically with reference to the reply document. As long as *registry status* for the reply document is R (see paragraph 6.2.3), the reference should be displayed in the relevant panels indicating that »Reply document is beaing created» or some similar indication. When *registry status* is changed til F, E or J, the reference should be displayed by way of document number (see K6.22). When *registry status* for the reply document is set to J, the depreciation is automatically completed through the filling-in of the following attributes and values on the received documents: • *Depreciation date*: date of reply document (from the attribute *Document date*). • *Mode of depreciation*: the value BU ("brev ut", i.e., outgoing letter) if the reply document is of type U, NN ("nytt notat", i.e., new memo) if reply document is of type N or X.	O

K4.42	In the enhanced version, it should be possible to carry out depreciation of document type N according to K4.40 - K4.41 for each individual addressee. This means that a received document may be depreciated for some addressees but not for others. Depreciation should not be registered on CC addressees.	O1
K4.43	It should be possible to depreciate documents of type I only with a document of type U. It should be possible to depreciate documents of type N with a document of type N, X or U.	O
K4.44	It should be possible to register documents of type U, N or X as preliminary replies to one or more received documents. The mode of depreciation for the received documents should be set automatically to ***. Later, when final replies are registered, the depreciation attibutes should be updated in accordance with K4.41-K4.42.	O
K4.45	Registry entries/addressees whose mode of depreciation is blank or ***, should be included in the arrears list, cfr. chapter 11.	O

Depreciation (and arrears control) is associated with individual registry entries (and addressees). It should, however, also be possible to complete an entire case by assigning the value A as *case status*. A completed case is locked for registration of new registry entries, but it should be possible to reopen the case by changing the status value. This is described in more detail in chapter 6.

K4.46	It should be possible to depreciate all non-depreciated documents in one operation by setting the *case status* to A. The mode of depreciation is then automatically set to A for all registry entries/addressees. Such collective depreciation should not be effectuated without requiring the user to confirm the operation, and the system should list the registry entries (and addressees) which will be automaticaly depreciated. Should the user choose not to depreciate all registry entries, the *case status* cannot be set to A.	O

If the case handling is paper-based, the executive officer or manager will be able to indicate on the document itself that it should be depreciated, and depreciation in the registry may be performed by the registry when the document gets there. If the case handling is based on electronic documents, this opportunity does not exist. In such cases, the executive officer/manager may carry out depreciation directly in the registry, or the registry may carry out depreciation after reply has been given. It may then be necessary to log who has carried out the depreciation, and possibly on behalf of whom. Such functions may also be useful if the recordkeeping is paper-based.

K4.47	The system should be able to log who has effectuated depreciation, and it should be possible to register that depreciation has been carried out on behalf of somebody else – see the table *Additional information.* Each organization should be able to choose whether this function is to be implemented or not.	O1

The depreciation attributes may also be used to check if outgoing letters have been replied to.

K4.48	It should also be possible to use the attributes *Depreciated by document*, *Depreciation date* and *Mode of depreciation* for document type U, to indicate that reply has been received for an outgoing letter. It should also be possible to associate a received reply (document type I) with the outgoing letter according to principles similar to those of K4.41-K4.42.	A

This kind of association between documents does not constitute depreciation in a normal sense. It is not linked with the arrears control and not subject to any kind of regulation.

4.2.8 Notes, logs and other additional information

The table called *Note* is created in order to register *notes*, and the table called *Additional information* in order to store *change logs* produced by the system as well as *activity logs* and other kinds of additional infomation associated with the processing of a case or a document.

Notes may contain any information relevant to the case/document, e.g., comments regarding the handling procedure, internal comments on the reality of the case/document, etc. Notes in electronic form may replace what is today scribbled on the documents themselves, on files, etc. This transition will be necessary when case documents no longer exist in paper form, but the opportunity may be used independently of how the case documents are stored.

K4.49	There should be functions for registering notes on cases, registry entries and documents, cfr. the table *Note*.	O2

Change logs are used when changes whose documentation is important, are made in the database. Requirements for change logs are part of the specifications. Examples of functions where change logs are required, are splitting up and combination of cases – see 4.2.4 above.

Storing *activity logs* is an issue primarily in situations where Noark is integrated in or with an electronic case handling system. Storing activity logs makes it possible to document the internal processing for posterity and improves traceability. One example of acitivity logs which are required in Noark, is the logging of who effectuates depreciation, cfr. K4.49 above. The organization itself must decide what activity logs to store.

The tables *Note* and *Additional information* are also used by the module for electronic recordkeeping, and are included in the technical description (paragraphs 14.2.30 and 14.2.31). This includes a more detailed description of what is to be logged.

4.2.9 Precedents

A decision of principal improtance is called a precedent. Precedents are normative for the processing of similar cases. If it is decided during processing that a specific case may constitute a precedent for similar cases later on, the executive officer or manager may decide that the case should be registered as a precedent. In this way, it is possible to build up a precedent register which may simplify decision-making. The table *Precedent* is created to register precedents.

Precedents are particularly important in connection with laws and regulations. They complement the regulations and contribute to secure equality in the processing of cases. For this to happen, the precedents must be known to the executive officer at the time of decision-making or preparation. In this context, a precedent register in or linked to a Noark system may be be an important working tool.

Even if it is customary to talk about precedent cases, it is usually one (or a few) of the documents which constitutes the precedent. Apart from registering the whole case, one must be able to identify the document(s) which contain(s) the precedent decision.

K4.50	It should be possible to register cases as precedent cases in a precedent register, cfr. the table *Precedent*.	O
K4.51	In the enhanced version, it should be possible to refer to one or more documents (registry entries) within a precedent case.	O1
K4.52	A precedent may to refer to cases in all parts of the Noark base.	O
K4.53	In the enhanced version, a precedent may also refer to cases which are not part of the base. It should, in such situations, be possible to include a text which describes the reference as exactly as possible.	O1

4.2.10 Disposal and preservation

Administrative bodies should have rules for the disposal of cases which are not to be preserved for posterity. Disposal means that records material is removed and destructed after having been kept in the records. In the context of Noark, this applies only to (case) documents. Records information and other information registered in Noark is usually not disposed of. Disposal must be authorized by the National Archivist through general or specific rules.

For paper documents, disposal means that the documents are physically taken out of the registry and destructed. In the context of electronic recordkeeping, disposal should as a minimum involve breaking the link between the registry entry and the document, so that the document is no longer available from the recordkeeping system, and so that it is not included during export from the records database. However, when documents contain sensitive information (according to professional secrecy, grading, etc.), it is necessary to follow the rules which apply to physical destruction of such documents.

In a disposal plan, disposal provisions (see *Disposal code and Preservation time*) may in some cases be associated with a specific order value (file code). Default values for disposal may therefore be specified in the table *Order value*, cfr. paragraph 14.4.9. The disposal code may for instance be K for "kasseres" (to be disposed of) or G for "gjennomgås" (to be reviewed) with a view to appraisal. In addition to the defined default values, other values may be specified. In the attribute *Preservation time* is specified the number of years it should take from the case is completed until it is disposed of. When a case is completed, the system should automatically calculate the time for disposal or appraisal, cfr. the attribute *Year of disposal.*

In the context of electronic recordkeeping, disposal of cases where the year of disposal has been specified, may be carried out in an automated operation. A summary of cases for disposal may be obtained by extracting a disposal list - see paragraph 11.3.7.

In the context of physical records, cases for disposal must be retrieved manually. As cases are removed from the records, the disposal code in the Noark base may be updated to U for "utført" (done). It is also possible to use the automated disposal function, but if this is done, it is recomended that the cases first be physically removed from the records.

For deletion of different versions of an electronic document, see chapter 6, K6.30–K6.33.

K4.54	It should be possible to register disposal code on a case, cfr. the attribute *Disposal code.* Permissible values should be registered in the table *Disposal code* or in a similar manner in advance. The values which are specified in Noark-4, are default values, but other values may also be entered.	O
K4.55	When the disposal code is registered for a case, it should be mandatory to specify the number of years it should take before the case may/should be disposed of or appraised with a view to disposal, cfr. the attribute *Preservation time.*	O
K4.56	It should be possible to configure the automatic filling in of *Disposal code* and *Preservation time* based on the file code (cfr. the disposal attributes in the table *Order value*).	A
K4.57	When a case is completed (*case status* set to A, cfr. chapter 6), *Year of disposal* is filled in automatically by the system. Its value is calculated by adding the year from the attribute *Last document date* to the number of years specified in *Preservation time*. In the event of a case being reopened, *Year of disposal* should be reset.	O
K4.58	There should be functions for searching for cases which have reached the time for disposal or appraisal, and possibly for effectuating the disposal.	O
K4.59	Disposal should be carried out as a semi-automated (the user being prompted for each individual case) or fully automated process. Only cases with a year in the attribute *Year of disposal*, i.e., completed cases, may be disposed of. (The report *List of disposal* lists the cases for disposal.) When disposal is effectuated, disposal code is changed to U and *Year of disposal* locked for changes.	O1
K4.60	Only authorized personnel (role 1 - AR1, cfr. K8.13) is allowed to effectuate the automated disposal function.	O1
K4.61	It should not be possible to dispose of a precedent case, even if it has been indicated that it is obsolete. If precedent has been indicated, the only permissible disposal code is B ("bevares", i.e., to be preserved) or blank.	O
K4.62	Disposal in the context of electronic recordkeeping should lead to the link (relation) being broken between the registry entries of the disposed case and its associated documents. Any links between such documents and *other* registry entries should be maintaied. If there are other links to such documents in Noark or an associated system, it should not be possible to delete the documents from the electronic document store. If no such links exist, it should be possible to delete the document.	O2

4.2.11 Automated functions

Some automated functions, such as assigning case number, associating case with records section, etc., are specified in various places in part I of this report. In addition, the following requirements apply with regard to automated functions (note that requirements with regard to automation are also specified in connection with the individual attributes in part 2, chapter 14):

K4.63	The following attributes should be filled in automatically and, if appropriate, updated automatically by the system: • *The number of registry entries* (table: *Case*) should be updated when a new record is registered. Not to be modified by the user. • *Last document date* (table: *Case*) should be updated with record date when a new record is registered. Not to be modified by the user. • *Case date* (table: *Case*) should be filled in with the current date at the time of case creation. May be modified by the user. • *Record date* (table: *Registry entry*) should be filled in with the current date at the time of record creation. May be modified by the user.	O
K4.64	The following attributes are obligatory, i.e., they must be filled in in order to store a case or a registry entry with its associated sender/addressee and any electronic documents: • Case title (table: *Case*) • Content description (table: *Registry entry*) • Sender/addressee • Authority to exempt from public access (all tables) – only if the registered access code is different from XX. • Document title (table: *Document description*) – only if the document is stored electronically.	O
K4.65	When a new registry entry is created, it should be possible to fill in the attributes by copying another record in the same case. The user should be able to modify the information.	O1
K4.66	When a registry entry is registered as a reply to a document (see K4.41), the following information should be retrieved automatically from the record to the received document: • Content description • The sender of the received document should be copied to addressee on the reply document • Document type should be set to U if the received one has type I; document type should be copied if it is N or X. The user should be able to modify the information.	O1
K4.67	If K4.48 is implemented, the system should offer functionality corresponding to that of K4.66 for incoming documents which reply to outgoing ones.	A
K4.68	It should be possible to copy *Case title* to *Content description* in a registry entry.	O
K4.69	The content description of a registry entry should, as default, be copied automatically to *Document title* in *Document description* (for electronic documents). The user should be able to modify the document title.	O2

4.2.12 Other functions

In addition to the functionality described above, the records management of Noark-4 should include the following:

- *Registering maturity and processing deadlines:* Maturity normally means the deadline the sender has indicated on a received dicument (document types I and N). Processing deadline is the deadline which the addressee (recipient) himself imposes. This may correspond to the maturity date or be independent of it. Thus, in cases involving several adressees (document type N), each addressee may impose his or her deadline.

K4.70	For document types I and N, it should be possible to register maturity date, cfr. the attribute *Maturity date* in the table *Registry entry*.	O
K4.71	In the enhanced version, the individual addressee should be able to register an internal processing deadline. It should be possible to copy this deadline from *Maturity date*, if it has been indicated, or to register it independently of this.	O1

- *Registering (re)activation date:* Activation date means a date fixed by the executive officer or manager for having the whole case forwarded from the registry. With paper-based recordkeeping, this should be combined with procedures where the registry retrieves any NB cases and makes sure they forwarded to the manager/executive officer. In the context of electronic recordkeeping, the most natural procedure would be for the executive officer to search for the case, or having a system that automatically forwards it through an internal system for document flow/case handling.

K4.72	It should be possible to register (re)activation date on cases in the attribute *NB.*	O
K4.73	If the recordkeeping system is integrated with a case handling system, the system should be able to search for NB cases with a given date automatically and log a message with reference to the executive officer.	S1

- *Registering loans:* It should be possible to lend out an entire case (file with all documents associated with the case) or single documents including any attachments. It should be possible to include the borrower and the loan date in the registration. Handing in is indicated by deleting the loan information. This function is of no interest if the case is stored electronically.

K4.74	It should be possible to register loans by filling in the attributes *Loan date* and *Lent to*. The registration might include an entire case (table: *Case*) or single documents including any attachments (table: *Registry entry*).	O

- *Registering dispatch and dispatch method:* For all types of documents, it should be possible to register the dispatch method for the various addressees, i.e., standard mail, fax, e-mail, etc. If the records are electronic, it must also be possible to register the fact that a dispatch (document and any attachments) has been effectuated, including date/time and sender.

K4.75	For each recipient of a document, it should be possible to register dispatch method (mail, fax, e-mail, etc.) – cfr. the attribute *Dispatch method* in *Sender/addressee*.	O1
K4.76	For each recipient of a document of type U, N, X or S, it should be possible to register the dispatch date and the initials of the person who effectuated the dispatch.	O2

Functionality related to dispatch by means of e-mail is described in more detail in chapter 10.1.

4.2.13 Linking up with other modules

The records management module is vital to the recordkeeping system and closely linked up with the other modules. The linking is as follows:

- *Access-control module:* All use of the system is subject to user management and access control as specified in the records management module - see chapter 8. This includes the users' right to register or correct as well as to search for and read information in the records management module. Some of these rights are associated with various stages in the decision-making process and managed by attributes in the tables *Case* and *Registry entry*. These are described in chapter 6.

- *Record structure module:* All the cases in the records management module are associated with an administrative unit, a registry management unit, a records section and entity of records. These structures are defined in the record structure module and described in chapter 7.

- *Electronic records:* Individual registry entries play a vital role as gateways to the stored case documents, be they hardcopies (on paper) or stored electronically. However, electronic storage and handling of case documents are maintained by the module for electronic recordkeeping, and this is also where the tables reside which maintain the relationships between registry entries and case documents, cfr. chapter 5.

- *Board-handling module:* When collegiate bodies (advisory and governing boards, etc.) take part in the decision-making process, the board-handling module is used to keep track of the document flow and work flow. However, the processing usually involves cases which arise and are completed in the records management module, and a considerable proportion of the board documents are registeres in the registry. Registered board documents such as drafts, minutes and opinions have special functions in the decision-making process, but as far as recordkeeping is concerned, they are on the same level as other registered documents. All the details concerning board-handling are described in chapter 9.

4.3 Procedure requirements

The basic procedures for entry into records and records management are described in the regulations[5] and established through 10-12 years of computer-based recordkeeping using Noark systems. It is therefore not considered necessary to present a complete description of such procedures here.

4.3.1 Prodecures related to special functions

Procedures related to new functions in Noark-4 are described in other chapters, e.g., in connection with the other modules. All of these are, however, closely related to the records management module:

- Chapter 6 describes the work flow and document flow of the decision-making process, both for paper-based and electronic recordkeeping and decision-making environments.
- Chapter 7 describes procedures related to the record structure of the organization.
- Chapter 8 describes procedures for access control.
- Chapter 5 describes procedure changes in connection with the transition to electronic recordkeeping.
- Chapter 9 describes procedures related to political decision-making and document handling in connection with this.
- Chapter 10 describes procedures related to the use of integrated e-mail and digital signatures.

In addition, it is worth paying attention to the following functions, which require set procedures:

- When registry entries are moved from one case to another (split or combined – see paragraph 4.2.4 above) and when documents within a case are renumbered, one must be careful to update the numbers on the associated paper documents in accordance with the changes that are made in the base.
- When sender and addressee are registered on documents, clearly defined procedures should be followed, even if Noark-4 provides for much flexibility. As a rule of thumb, the addressee for incoming letters (type I) should be the organization itself (system default). The internal distribution is maintained by registering administrative unit and case-responsible/executive officer. Likewise, the sender for outgoing letters (type U) should normally be the organization itself (system default). The need to register several addressees and senders is mainly restricted to the following:
- Several recipients of an outgoing letter (type U)
- Several recipients of an internal document (types N and X)
- Internal and external CC addressees of all types of documents
- Several senders on a received document (type I, N or X) - preseumably happens rarely
- Procedures for handling internal documents are closely related to the record structure, and are dealt with in chapter 7 (7.3.2)

[5] Arkivforskriften (the Archives Regulation), cfr. kgl.res. (royal decree) 11.12.1998.

4.4 Essential tables in the module

For a complete list of tables and attributes, see chapter 14.2.

Table name	Text
Case	Contains information which identifies a case (case number and title) as well as information common to all documents within the case.
Registry entry	Contains information which describes the documents in the individual cases (cfr. the document record of Noark-3) as well as information regarding processing and status.
Sender/addressee	Makes it possible to register more than one sender/addressee for a document. Contains name, address, etc., of sender/addressee, as well as information on executive officer, decpreciation and dispatch. This provides for varied follow-up of the decision-making process for various recipients (particularly important for internal documents).
Notes	Contains notes (remarks) on a case, a registry entry or a version of a case document. This could be a comment on the processing itself or comments or corrections regarding the contents of the case or the document.
Additional information	Contains various kinds of additional information on a case, a registry entry or a version of a case document. The main types of additional information are: • Processing information (activity log) • Change logs, etc.
Filing plan code	Contains assigned values in terms of subjet (topic) codes or object codes. The code is specified as primary, secondary, tertiary, etc., if it is used as an additional filing plan code.
Part in case	Contains information (name, address, etc.) which describes the internal unit(s), external organization(s) or private person(s) who is/are part(s) in the case.
Confer case	Contains references from one case to other cases, single documents within these cases and cases in the precedent register. Is used to link references between cases.
Precedent	Contains information on precedent cases.

4.5 Changes from Noark-3 and Koark

Below is given a brief summary of changes in the records management module as compared to Noark-3 and Koark. A complete specification of all differences is given in chapter 16, which also discusses compatibility and conversion opportunities.

Basic version (requirement type O):

- The concept of *records management* is new. The *module for registration and records management* in Noark-4 corresponds to the *registry section* of Koark, while the entire Noark-3 is defined as a computer-based *system for entry into records.*
- The concept of *Registry entry* (table) replaces *Document (register).*
- The concept of *Content description* (attribute) replaces *Document description*.
- The concept of *Access code* (attribute) replaces *Grading code*, cfr. ch. 8.
- The concept of *Processing deadline* (attribute) is introduced, as well as *Maturity.*
- To case number, document number and serial number has been added an extra digit.
- The record structures has been modified somewhat. This has consequences for registration of records references (entity of records, records section, etc.). The record structure permits several types of filing plans (state plans, K codes, etc.). This is in accordance with Koark, but in enhanced versions the technical solutions are modified, as discussed below. The new record structure is described under the record structure module (chapter 7).
- The *Cross reference* field has been omitted. The functions covered by this field have been replaced by two new attributes: *Project* and *Confer case.* See also the previous indent on record structure, as well as below on file codes in the enhanced version.
- The functionality related to *disposal* and *precedent* has been enhanced.
- The screening codes under *grading* have been replaced by functions for checking off the information to be screened off, cfr. chapter 8.
- The attribute *Case status* has been kept from Koark, and is not found in Noark-3.
- The *Doc no.* field under *Depreciation* is replaced by two attributes: *Depreciated by document* and *Replies to document*.

Enhanced version (requirement type O1):

- The concept of *Registry status* (attribute) replaces *Document status* (Koark).
- There are attributes for registering an arbitrary number of file codes. These may be ordered hierarchically (primary, secondary, tertiary code, etc.) or be independent (e.g., additional codes), cfr. record structure in ch. 7.
- Registering administrative units – see *Case-responsible* and *Executive officer* – is much more flexible, see chapter 7.
- Some attributes have been omitted from *Registry entry* and moved to a separate table, S*ender/addressee.* This provides for registering several sender/addressees on one and the same document, and for separate follow-up of internal documents with individual recipients.
- A new table has been created for registering parts in a case - *Case part.*
- A new table has been created for storing change logs and other additional information - *Additional information.*

Electronic records (requirement type O2):

- The fields for references to electronic documents have been omitted and replaced by more comprehensive functionality for electronic recordkeeping - see chapter 5.

- A new table has been created for registering notes - *Notes.*

Recommended functionality (requirement type A):

- A case may be divided into several *case sections*, as discussed in chapter 7.

5. MODULE FOR ELECTRONIC RECORDKEEPING

5.1 Purpose of module

The purpose of this module is to link the records management module to electronic documents which constitute case records. Even before Noark-4, it was possible to link electronic documents to registry entries, but the specifications of Noark-3 and Koark were on a general level. Besides, the archival copies were meant to be in hardcopy (paper). As from Noark-4, it is possible to make the transition from paper-based to electronic recordkeeping. The module for electronic recordkeeping should, however, be able to handle a situation where some of the case records are still in paper form.

The relationship between this module and the rest of the system is shown in figure 5-1.

The electronic records must contain the same types of documents as those which are currently stored in paper form: text documents, construction sketches, maps, pictures, etc.

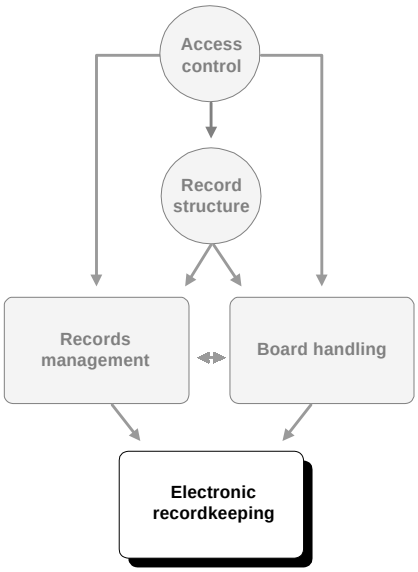


Figure 5-1: Module for electronic recordkeeping in Noark

Electronic case records should fulfil the same role as traditional paper-based records; they should, among other things:

- provide information to executive officers for use in the handling of cases
- document for posterity the processing that has been done

However, electronic recordkeeping provides new opportunities:

- The case documents are immediately made available to the workstations of the executive officers. This will replace traditional distribution and lending.
- The contents of the stored documents may be re-used in new text production.
- It is easier to give the public insight into ungraded documents.

However, electronic recordkeeping as opposed to traditional, paper-based recordkeeping, also entails some problems and challenges which this module need to address:

- The documents must be readable and available even in the future; this is made more difficult by a multiplicity of production formats which are frequently released in updated versions.

- In connection with periodization and reorganization, it must be possible to export the documents for storage in an archival repository together with its associated registry information.
- It must be possible to guarantee that the documents are authentic (not forged).
- In a paper-based entity of records, corrections, notes, etc., on the drafts may provide valuable information on the processing of the case, and there should be mechanisms which preserve this kind of information.

5.2 Module design

It may be useful to start off by clarifying how this module relates to the records management module and take a closer look at the types of documents which may be eligible for storage as electronic records.

5.2.1 How it relates to the records management module

The documents in the electronic records should be linked to the registry entries of the records management module. This is the starting point for searching for registered electronic documents, and this is where the access rights for these documents are managed. Thus, the records management module is the gateway to the case records, be they paper-based or electronic.

K5.1	All stored documents in the electronic case records should be subject to Noark's records management. All access control is managed from here.	O2

In Noark-3 and Koark, it has been possible to associate a single document with a registry entry. Noark-4 should allow more than one document to be associated with the same registry entry. There may, for instance, be one main document and several attachments. It should, furthermore, be possible to associate a document with several registry entries, for instance as a main document in one registry entry and as attachments in others. This would prevent multiple storing of documents in the electronic records and ensure that the document appears as identical in all contexts as well as guaranteeing uniform access rules for the document in question.

K5.2	A registry entry may refer to more than one document. Only one of these may constitute the main document.	O2
K5.3	A document may be associated with several registry entries. However, it may constitute a main document only in one of these.	O2

5.2.2 Versions, variants and formats

In paper-based records, it is common to store drafts with their scribbled corrections, notes and authorizing signatures (initials) from the responsible executive officers at various steps and levels of the processing. This may provide valuable information on processing and evaluations that have taken place. In the context of electronic recordkeeping, it is often desirable to have several *versions* of a document (draft) in order to identify what has been done and authorized by whom during the processing. Separate versions addresses the need

for guarantee of integrity. The case handling system may be designed so as to preserve all or selected versions of a document.

In a *recordkeeping system*, one may choose to store only the final (finalized) document. However, Noark-4 should also provide for the storage of previous *versions* of a document when this is significant in order to document the processing. Common practice from paper-based recordkeeping may be perpetuated in Noark-4 in a modified form.

Any electronic document is from the beginning stored in a technical *format* determined by the tool used to produce the document. If many different tools are used, for instance one or more text editors, spreadsheet applications, graphics applications, etc., the result will be records consisting of an infinite variety of different formats. It must be possible to convert these formats into a few standardized *archival formats* suitable for long-term storage. This is discussed in more detail in paragraph 5.3. However, even when a document has been converted to such an archival format, it may be desirable to preserve the original *production format*, e.g., in order to reuse text. For this to be possible, a document must exist in both an archival format and the production format, possibly in both formats simultaneously.

In Noark-4, it should also be possible to store public versions of documents which are exempt from public access. Likewise, it should be possible to store documents to which digital signatures have been applied, as separate editions. In the latter case, there may for instance be solutions where both the document itself, the signature and the signature certificate are stored in the same file (see paragraph 10.2). Noark refers to such public and digitally signed copies of a document version as *variants* (in practice, however, it is often natural - and unproblematic - to refer to them as "versions"). A *variant* is subordinate to an ordinary (and usually final) version of a document, and is always stored together with this.

Figure 5-2: Versions, variants and formats

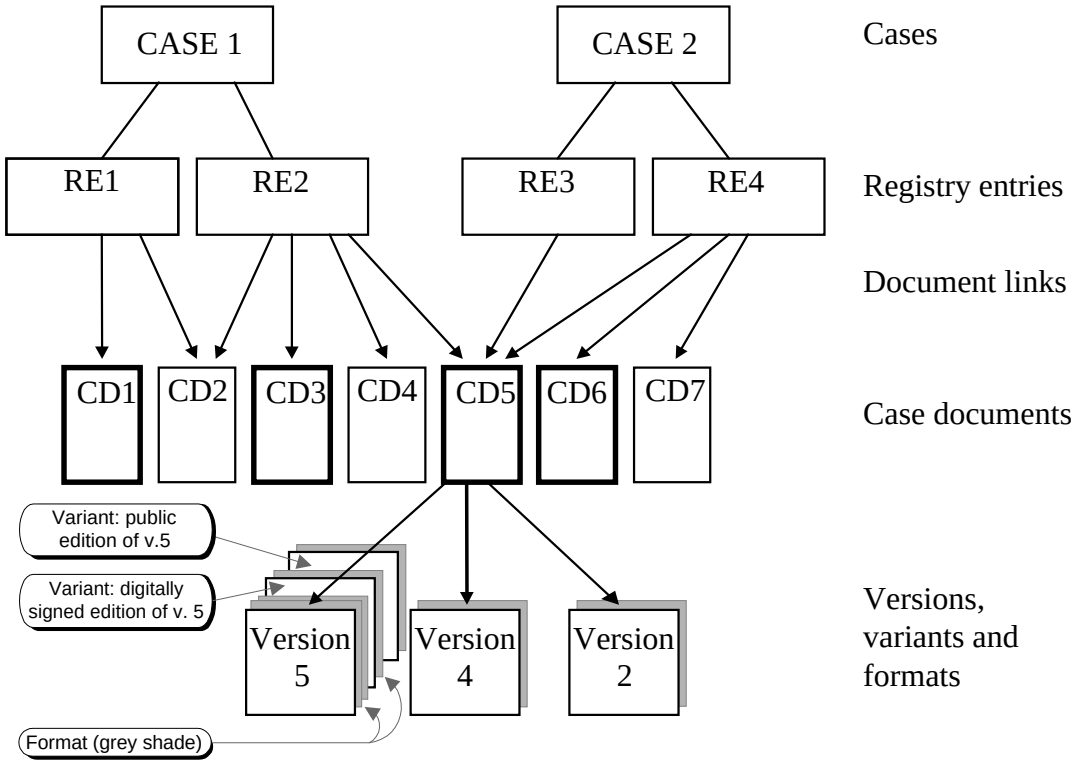


Figure 5-2 illustrates the relationship between cases, registry entries and formats. The figure shows an example of how case documents may be associated with one or more registry entries within the same case or belonging to several cases. Main documents are indicated by heavier outlines. This example also shows how a case document may exist in several versions, variants and formats.

- Case document CD1 is only associated with registry entry RE1 as a main document.
- Case document CD2 is associated with both registry entries RE1 and RE2 as an attachment.
- Case document CD3 is only associated with registry entry RE2 as a main document.
- Case document CD4 is only associated with registry entry RE2 as an attachement.
- Case document CD5 is associated with registry entry RE3 as a main document and with RE2 and RE4 as an attachment.
- Case document CD6 is only associated with registry entry RE4 as a main document.
- Case document CD7 is only associated with registry entry RE4 as an attachment.

Case document CD5 has three stored *versions*: 2, 4 and 5. The abscence of versions 1 and 3 from the records would normally indicate that they are not considered to be of archival value and have thus been deleted, or that they have not been transferred from the case handling system. Versions 2 and 4 are drafts to be preserved, whereas version 5 is the final version of the document.

Version 5 also has two *variants*: one public and one digitally signed edition.

All versions and variants are stored in a *format* (shaded grey in the illustration). The figure does not distinguish between archival formats and production formats. It does, however, indicate that version 5 has been stored in two formats, i.e., both in archival format (e.g., PDF) and production format (e.g., Word97).

K5.4	It should be possible to store a document in several versions which reflect different stages of the development towards the final document.	O2
K5.5	It should be possible to store the same version of a document with several associated ”variants”, i.e., alternative editions of the version which have had digital signatures applied to them or been specially adapted for public use.	O2
K5.6	If a document is stored in several versions and/or variants, this should appear clearly from the relevant panels.	O2
K5.7	It should be possible to store the same *version* both in the production format and in an archival format (format for long-term storage). It should be possible to store a *variant* either in the production format or in an archival format.	O2
K5.8	If several formats exist for a document (or a version of a document), this should appear clearly from the relevant panels.	O2

5.2.3 Paper-based vs. electronic recordkeeping

Noark should be able to handle *both* paper-based and electronic storage of documents. Noark allows for combined storage of cases with paper documents and cases with electronic documents. Normally, however, all *main documents* within a case should be

stored electronically in order for the case to be considered as electronically stored. If this condition is not satisfied, the entire case must be stored on paper. Any electronic documents which may exist within such a case, are regarded as work (copy) versions.

The *Case* table should contain an attribute called *Stored on paper*, which shows whether the case documents are stored in paper-based or electronic form. If this attribute has a value which says that the case is stored electronically, then the system should automatically check that all *main documents* within the case have been stored in electronic form.

In electronically stored cases, all attachments *ought to* be stored electronically as well. It is, however, permissible to store certain attachments, such as extensive reports, on paper. In such cases, the system must contain a clear reference to the location of the paper-based attachment. The attribute *Archival note* in the table *Version* (see paragraph 14.3.3) is used to refer to the paper document.

In addition to this, it should be possible to store a large *main document* in an electronic case on paper if the first page is scanned or a reference document inserted instead of the main document. The existence of a paper-based archival copy is identified through a front-page marker where the attribute *Association code* in the table *Document associtation* has the value "FH" (see paragraph 14.3.9).

Procedures relating to electronic recordkeeping are described in more detail in paragraph 5.5.2.

K5.9	The system must distinguish between cases where the official and valid documents are stored on paper, and cases where they are stored electronically.	O2
K5.10	If a case is stored electronically, the system should check that all *main documents* which belong to the case, are also stored electronically.	O2
K5.11	Even if a case is stored electronically, the system should allow for *attachments* to be stored on paper. The system must provide a unique reference to the physical location of the attachment.	O2
K5.12	The system should also provide for substituting a reference document which refers to an archival copy on paper, for a main document in an electronically stored case.	O2

5.2.4 Module design

The main tables of the module are *Document link*, *Document description* and *Version*. The following figure shows how the tables relate to each other. Tables residing in other modules are in grey shade.

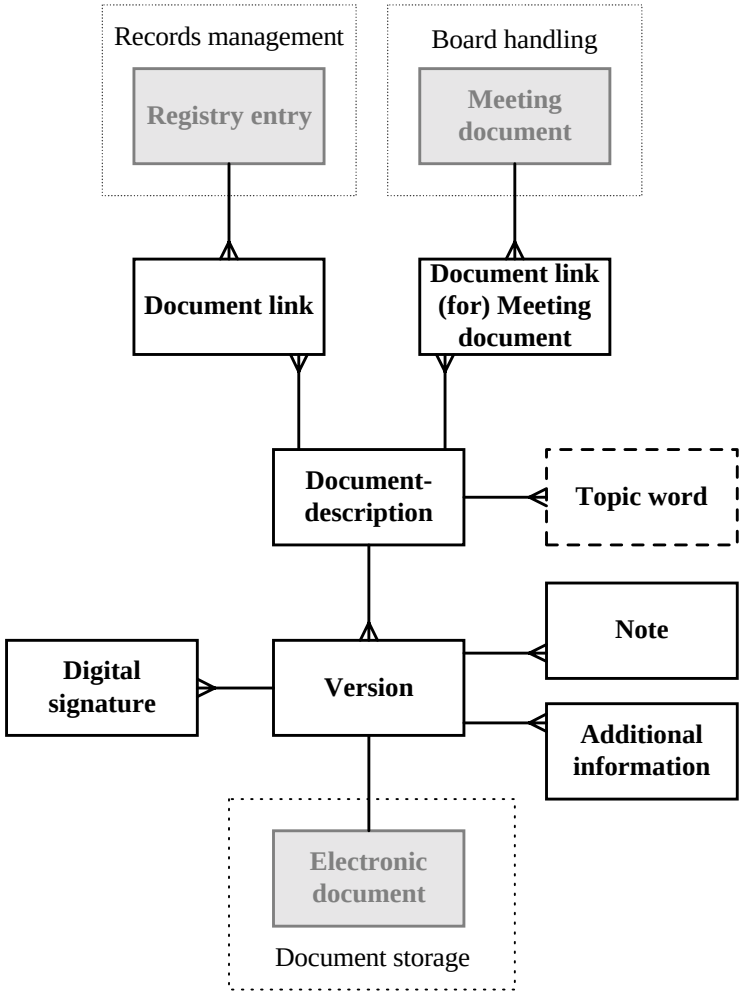


Figure 5-3: Electronic recordkeeping - simplified data model

Brief description of the contents of the above tables:

- *Document link* (cfr. paragraph 14.3.1): This table is introduced in order to dissolve the M:M relationship between registry entries and documents. A document may be associated with the registry entry as a main document, a dispatch letter, an attachment, etc. Thus, there must be an attribute in this table which shows what kind of association we are dealing with. One of the documents must always be the main document.

  There is a similar association between the electronic records and the board-handling module, called *Document link meeting document* (cfr. paragraph 14.6.6). From the board-handling module, reference may be made to the board documents which are not entered into the records, and which are thus not referred to from the records management module. These may for instance be minutes, which constitute a separate series within the records. Board documents are discussed in connection with the board-handling module in chapter 9.

- *Document description* (cfr. paragraph 14.3.2): All electronically stored documents should be linked to this table. According to SGK specifications, there should be an equivalent table in the case handling system. If the case handling system is integrated with Noark, the contents of several of the table's attributes will normally be registered from the case handling system, such as *Document title* and *Document category* (letter, memo, report, etc.). Such registration of information in Noark is primarily carried out in connection with attachments. The relationship between electronic records and SGK is described in more detail in paragraph 5.2.6 below.

  The attribute *Document status* in the table *Document description* is a "flag" which shows if documents are being produced (status B) or if they have been processed by the executive officer (status F). The use of status values during document production is part of Noark's process management and is described in more detail in chapter 6.

  It should be possible to assign an access code to an attachment that is different from that of the registry entry. For this reason, the table *Document description* must contain the attributes *Access code* and *Access group* - as well as the attributes *Authority to exempt from public access*, *Date of downgrading* and *Downgrading code*.

- *Version* (cfr. paragraph 14.3.3): It must be possible to store a document in several versions, and to store a version in several formats. Information on versions and formats are stored in the table *Version*. There is a 1:M relationship between *Document description* and *Version*. The *Version* table also constitutes the interface to the electronic document itself, and there is a 1:1 relationship between the two.

  One of the attributes in the *Version* table is *Version number*. The last version of the document has the highest number. The version number must be combined with another attribute called *Variant*. This shows what edition or what format of the version the individual registry entry contains. Permissible values for *Variant* are production format (P), archival format (A), signed document (S) and public version (O). If a specific version consists of several variants, the same version number may occur more than once. The document format (Word 6.0, TIFF 6.0, PDF, etc.) for the version/variant should be registered (automatically) in the attribute *Storage format*. Based on this, the records entity should check that documents are stored in an archival format (A).

- *Note* (cfr. paragraph 14.2.30): It has been described how several versions of the same document may contribute towards documenting the processing. However, it is also necessary to document the processing by other means. It should be possible to register comments and remarks directly related to a document in the same way that we register notes on cases and registry entries. It should be possible to link notes to the tables *Document description* and *Version*, and there should be a 1:M relationship between these and the table *Note*. The text which constitutes the note, is registered in a separate attribute called *Note*, and this should be so designed as not to impose any length restriction on the registered information.

  Primarily, all notes should be registered in the attribute *Note*, but it should also be possible to link electronic documents to the note. These may, for instance, be hand-written notes that have been scanned. There should, therefore, be a 1:1 relationship between *Note* and the table *Document description*.

K5.13	It should be possible to link one or more notes of arbitrary length to any document or document version.	O2

K5.14	It should also be possible to use scanned documents as notes.	A

Digital signature (cfr. paragraph 14.3.4): During exchange of e-mail, digital signatures may be used to verify the authenticity of documents (ensuring the addressee of the identity of the sender) as well as their integrity (that the contents have not been modified). Digital signatures may also be used for guaranteeing the authenticity and integrity of documents which are filed in the electronic records. The signature must then be applied to the document after this has been converted into an archival format.

In Noark, it should also be possible to file documents with digital signatures and their associated certificates as a separate variant S. Such documents will then still be verifiable. It should, furthermore, be possible to store signatures and certificates in a separate table: *Digital signature*. In this table, it should also be possible to store information such as who verified the signature and when. This preserves traces of signatures and verification even in cases where opportunities for further verification are lost. There is a 1:M relationship between *Version* and *Digital signature*.

Digital signatures and e-mail is described in more detail in chapter 10, cfr., in particular, the requirements formulated in K10.36 - K10.53.

- *Additional information* (cfr. paragraph 14.2.31): The system should automatically log certain information in connection with the electronic storage of a document. This applies to the filing time and who carried out the filing. Likewise, information should be logged with regard to when the document was converted into an archival format and who converted it. Such log information is stored in *Additional information*. Both *Document description* and *Version* are linked to this table in a 1:M relationship. Even *Case* and *Registry entry* are linked to the table *Additional information* (see part II, Technical specifications, for a closer description of how the log function may be implemented).

K5.15	The system should log the filing time and the person who carried out the filing.	O2
K5.16	The system should log the time when a document was converted from its production format into an archival format, as well as the person who carried out the operation.	O2

5.2.5 The electronic document storage

Noark-4 does not specify how documents are to be stored and organized in the electronic document storage. The documents may be stored in tables in a database system, or as individual files in a file system. It is up to vendors to choose an appropriate solution. The chosen solution must, however, support the export of documents to individual files as decribed in paragraph 5.4.

Vendors must also decide if documents are to be stored in the same system as the registry information (Noark), or if they are to be stored in a separate system. If Noark is integrated with a case handling system, it seems natural that the two systems share a common document storage. However, irrespective of the solution selected, the individual electronic document should be linked to the table *Version* in a 1:1 relationship.

5.2.6 How it relates to SGK

Electronic document storage is thoroughly discussed in the report *Elektronisk saksbehandling. Statens generelle kravspesifikasjon* [Electronic case handling. General specification of requirements for the state administration] (Statskonsult 1997). This report presupposes that all documents which executive officers need in order to perform their task, should be available from a common document storage. Many - but by no means all - of these documents are registered documents (case documents). The storage also contains previous versions (drafts) of finished and registered documents, and there may be notes, reports and any kind of collected information which executive officers must have access to, but which are not to be entered into records.

SGK, like Noark, presupposes that all documents are linked to a document decription. If the case handling system is integrated with Noark, this document description may be a table which is shared by the two systems. However, if a solution with separate tables is chosen, there must be mechanisms which automatically copy information from one table to another.

In a case handling system, one may choose to register a topic (subject) word and selected keywords when documents are produced. It should also be possible to search for these keywords from the records management system.

Electronic document storage provides for free-text searching in the documents, and in the case handling system it should be possible to retrieve documents by searching in the document text itself. It should also be possible to perform free-text searches from Noark.

K5.17	It should be possible to search for registered keywords and topic words in the document secription of individual electronic documents.	A
K5.18	It should be possible to do free-text searches in the documents of electronic records.	A

5.3 Document formats

5.3.1 Production formats

Documents may be stored in a number of different formats. By document format is understood the way in which characters, structures and layout are coded and organized. The original format of the document depends on the tool used to produce it. In Noark-4, such an original format is referred to as the *productin format*.

These formats may be divided into different categories, the most important of which are:

- character formats where only the characters (letters and numbers) are stored
- text formats which also preserve the structure and layout of the document
- graphics formats for storing pictures (often subdivided into raster graphics and vector graphics)

- video formats for storing "moving pictures"
- audio formats
- multimedia formats which combine text, layout, graphics, video and audio

The two most important formats for Noark-4 are text formats (produced by text editors) and raster graphics (scanned paper documents). Vector graphics may also occur (e.g., illustrations produced using CAD/CAM tools). Graphics elements are frequently pasted into text documents, e.g., as letterheads and logos. There may also be formats which are difficult to fit into the above categories, such as spreadsheets and digital maps.

Many of these production formats are so-called proprietary, i.e., they are specific to an individual vendor. In many cases, they are not openly documented. To read such a format, we must often use the same tool that was used to produce it. In many cases, we must also have the same version of the tool to be able to read the document. New versions are typically released frequently, which means that what is apparently one and the same format, is continuously changing. There are, admittedly, several "viewers" on the market which can read (but not edit) a number of formats, but there are hardly any viewers that can read all pertinent formats. Furthermore, viewers must be constantly upgraded in order to be able to read the latest versions.

The result of this development of continuous change will be that many organizations will not be able to read their own text files which are more than 5-7 years old. If availability is to be maintained, these must be constantly converted into newer versions. And if we still store many different formats, this converting job will grow out of proportion and quality control will be very difficult.

One of the problems is the limited durability of electronic storage media such as tapes and CD's. However, the development of formats and software is a much more critical factor than the period that data may be stored intact on a certain medium. The need to convert into new formats will occur far earlier than the need to copy to a new medium due to limited durability.

When electronic documents are transferred to state or local depot institutions, these institutions take over responsibility for maintaining the availability of the documents. If they were to receive a multiplicity of document formats, the situation would be impossible to handle. It goes without saying that they cannot be expected to possess all the software (in the correct versions) that was used to produce the documents transferred to them. Long-term storage in a proprietary format is out of the question for the depot insitutions. The solution must therefore be to find one or a few stable and universal formats.

5.3.2 Archival formats

A precondition when storing case documents electronically - without, at the same time, storing the paper printouts of those documents - is that the availability of the documents is maintained for a long time. This is a fundamental requirement. It affects something as fundamental as the possibility of maintaining Norwegian administrative practice. The opposite would be a situation where the public administration wipes out its own traces, an administration where documentation and the general public's right to information is limited to a few years.

It would be possible to maintain availability for some time if the documents could be converted to a *standardized format*. Such a format must be openly documented, and preferably approved as an ISO standard. Standardized formats may be read across computer platforms and operating systems, and many of them have been developed for use as exchange formats. Such standardized formats are hereafter referred to as *archival formats.*

Not even an approved and well-established standard is guaranteed to last forever. Even standards have their generation gaps. Even if we select a certain standard as archival format, we must be prepared for later conversions, but such conversions will occur less frequently, and they will presumably be less risky and more complete than conversions between arbitrary production formats or between versions of the same format.

A Noark system with electronic records should have functions for converting between production formats and archival formats. This function should be easy to use. It should provide for converting individual files as well as for "mass conversion" of major parts of the document storage as batch jobs.

The conversion process must maintain the integrity of the documents. The basic requirement is that the contents (the "text") are rendered exactly as in the original document. It is also desirable to maintain the look and layout of the original document. Conversion into certain formats will result in losses of parts of the visual integrity, and conversion into plain text will lose any formatting that existed in the document.

It should not be possible to edit a document that has been stored in an archival format. This is a security feature that must be built into the system. It is described in more detail in chapter 6. However, even if a document is locked and cannot be edited, it will still be possible ro reuse text (from a number of formats) by cutting and pasting.

It should, if desired, be possible to store the same version of a document in both the production format and the archival format. The reason may be a wish to have access to all the edit functions of the production format. For long-term storage, it usually suffices to keep the archival format. During transfer to archival depot, it is usually the archival format that is transferred.

K5.19	It should be possible to convert documents from the production format to a standardized and openly documented archival format	O2
K5.20	The document conversion function must be easy to use.	O2
K5.21	It should be possible to convert documents individually and in batches.	O2
K5.22	The conversion should maintain the integrity of the document contents and preferably also the visual integrity of the documents.	O2
K5.23	A document which has been stored in an archival format, should be locked in order to impede any further editing.	O2

5.3.3 Archival formats approved in Noark-4

Noark-4 poses the following requirements for a suitable archival format:

- The format should be openly documented.
- It should preferably be an ISO standard
- It must be supported by complete and well-established products in the market.
- Converting documents to the archival format should be easy.
- It should be possible to convert to the archival format in question from most commonly used production formats, even from graphics formats (graphics elements should be included with the text).
- It must be possible to convert the archival format into new formats later on.

The development of standardized document formats has not yet reached a "mature" stage, and probably will not do so in the foreseeable future. As far as richly formatted documents are concerned, we lack well-established and broadly useable ISO standards. Ambitions must therefore be lowered when selecting a format. It will be necessary to reconvert archival documents later on, possibly on a regular basis. This makes it all the more important to reach a complete decision as far as formats are concerned. Later conversions will then not have to start from an impenetrable multiplicity, but may be carried out in manageable batches.

Which archival formats may be used in public administration is decided on the basis of the Archives Act, and the authority is vested with the National Archivist. Special provisions with regard to formats are expected to be prepared on the basis of the Archives Act, which entered into force on 1.1.1999. For the time being, there is reason to believe that the following formats will be accepted:

K5.24	It should be possible to use four archival formats for long-term storage in state or local originating organizations and for transfer to archival repository: • Text only: ISO Latin-1 8859-1:1987 • SGML - ISO 8879:1986, *including subset formats HTML and XML* • TIFF, version 6 • PDF	O2

5.3.4 Text only - ISO Latin-1 8859-1:1987

ISO Latin-1 is not strictly a document format, but rather a character set. However, it is simple to handle, and it will most likely be available in the foreseeable future. ISO Latin-1 can represent 256 symbols. The first 128 characters are identical to what is normally called ASCII (American Standard Code for Information Interchange). This includes upper- and lowercase letters from A to Z, as well as the numbers (digits) from 0 to 9 and some special characters such as period, comma, colon and semicolon. A few formatting codes (of which line feed and carriage return are the most important) are also defined. The letters Æ, Ø and Å as well as letters with accents are defined in the second half of the character set. In this second half, ISO Latin-1 differs significantly from what we normally know as ASCII.

Formatted documents which are converted into ISO Latin-1 will lose their structure and layout, and graphics cannot be represented in this format. However, the document contents - or text - are maintained. Thus, ISO Latin-1 is best suited to e-mail which is plain text, as well as notes and simple memos which are considered to be of archival value.

It is worth noting that ISO Latin-1 is also contained in other types of formats, such as SGML.

5.3.5 SGML (Standard Generalized Markup Language) - ISO 8879:1986

SGML was originally conceived as a standard for the printing industry. This standard defines the structure of a document and maintains all the structural editibility of the document across platforms. Standard SGML does not, however, handle layout.

SGML is strictly speaking not a format but a syntax (in the form of "markups" or "tags") for defining a specific application. The export format for tables and attributes in Noark is based on the same syntax. The setup and meaning of the syntax used in an SGML document must be further defined in a separate document template - a DTD (Document Type Definition). The document layout may be described in a DSSSL (Document Style Semantics and Specification Language).

K5.25	During export/transfer of SGML documents, an associated DTD must be included, as well as any associated DSSSL.	O2

The character set used in SGML should be ISO Latin-1. Graphics cannot be converted into SGML, and graphics elements cannot be built into the format. SGML may, however, contain references to separate files containing graphics, or to other external files. Noark should also be able to handle such complex documents. However, the remaining three archival formats selected for Noark may for the time entail considerable restrictions in terms of filing of complex documents.

HTML (Hyper Text Markup Language) may be regarded as an SGML application (a complete defined and fixed SGML code page). Thus, an HTML document needs no DTD. XML (Extensible Markup Language) is a subset of SGML (“SGML light”). Like SGML, it is a meta-language. Unlike HTML, it can be extended, and it allows the user to define a syntax. Even XML documents need a DTD. It may be an integral part of the document, in which case it constitutes the first part of it. It may also be included as a separate file, in which case it is handled and stored as for SGML documents.

For complex HTML and XML documents, Noark's requirements in terms of archival formats may impose the same restrictions as for SGML documents.

5.3.6 TIFF (Tagged Image File Format), version 6

TIFF is the most widespread and standardized raster-graphics format. It is the most widely used format for scanning paper documents. The format is portable across technology platforms and openly documented. It has recently been approved as an ISO standard (ISO 12639: 1997).
Raster graphics renders the document photo-identical, but it cannot be edited. There is, however, software which can convert from graphics to text format, so-called OCR software.

K5.26	TIFF files may be either ”multiple page” or ”single page”. If *single*	O2

	page is used, each single page of the document must be stored in a separate file in the same directory.	

With graphics formats, the biggest drawback is the vast amount of space taken up by the documents - up to 10 times that of a text format. Graphics formats are therefore not suitable for e-mail exchange. On the other hand, it is quite common to compress TIFF files. Compressing in Noark should be "lossless", i.e., it should not result in a permanent qualitative deterioration of the document.

K5.27	For compressing TIFF files, only the following standards are approved: • CCITT group 4 (for documents in black and white) • LZW(for documents with colours/shades of gray).	O2

5.3.7 PDF (Portable Document Format)

PDF is a non-editable format (printing format) which handles both text and graphics. Everything that can be printed on a printer - including all the other archival formats - can be converted and stored as PDF files. Scanned documents (e.g., in TIFF format) may thus be converted into PDF, and the size is considerably reduced. The visual integrity of the documents is maintained after conversion. The format cannot be edited, but it is possible to re-use text by cutting and pasting, because pure text is used internally in the format.

PDF is portable across platforms and openly documented, but it is not an ISO standard, as it is controlled by the vendor, Adobe. Still, PDF appears to be the most versatile and useful archival format existing today. None of the other archival formats can compare to PDF when it comes to commercially available solutions and products.

K5.28	PDF files with text should be stored in a character-based form, not in binary form, in cases where it is possible to choose between the two options.	O2
K5.29	When PDF files are compressed, only "lossless" compression should be used: CCITT group 4 or LZW.	O2
K5.30	It is recommended that PDF documents be stored so that the fonts that are used, are embedded in the documents. The documents will then take up (sometimes considerably) more space, but this will ensure that the fonts that are used, are kept in typographically identical form across platforms and time.	A

5.3.8 Exchange formats

Documents which arrive by e-mail, are electronical from the start. The e-mail itself is transferred in a text-only format, and might enter straight into the document storage. In addition, other file types may be sent as attachments to an e-mail. It is presumed that electronic case documents are normally sent as such attachments to e-mail. These attachments may be in any format. In most cases, they will be word processor files. The format that is used in attachments to e-mail, is referred to here as *exchange format*.

There is also a need for standardized formats for exchange of electronical documents within public administration. It cannot be taken for granted that the addressee is able to read the format used by the sender. Noark does not have rules for regulating this, but the sender should always make sure the user is able to read the document he/she sends (cfr. ch. 10).

It should, nevertheless, be noted that there are several advantages if the exchange format is identical to the archival format of the addressee:

- The addressee will always be able to read the document and have it displayed in a version identical to the archival copy of the sender.
- The addressee may file the document as it was received, without having to covert it.
- A recevied document with a digital signature may be filed by the addressee with its signature intact. If, on the other hand, the addressee must convert the document to an archival format, the signature will be "broken" and no longer verifiable.

5.4 Export and transfer of documents

There must be functions for exporting documents from the electronic records to a system-independent format. Such export will make it easier to convert (move) the documents when a new system is simplemented. Before reorganization takes place, all documents are to be removed from the database, exported in an *archival format.*

If a document consists of more than one file, all the files should be in the same directory. The system itself must handle references between the internal files in a complex document.

The standard medium for *transfer* to state or local archival repository is currently 74-minute CD-R discs (Compact Disc Recordable). The *file and directory structure* should conform to the ISO 9660 standard for maximum portabilty between technological platforms.

Document export must be carried out simultaneously with other export of selected attributes and tables from the system. The *Version* table represents the connection between the electronic documents and the rest of the system. Export from this table should contain the file name of the associated export documents.

The export format is described in more detail in the technical specifications in paragraph 15.3.4.

K5.31	It should be possible to export documents in archival format in the electronic records to individual files.	O2
K5.32	If a document consists of several files, all the files should be in the same directory.	O2
K5.33	DTD's and shared template files should be registered as documents in the tables *Document description* and *Version*.	O2
K5.34	The standard medium for *transfer* to state or local archival repository is currently CD-R disc (74 minutes). The file and directory structure	O2

	should conform to the ISO 9660 Level 1. File and directory names should thus contain up to 8 characters. Valid characters are limited to A-Z, 0-9 and Underscore ("_"), all in upper case (capital) letters. File names may have a 3-character extension. The directory structure may consist of up to 8 levels. Alternatively, the file and directory structure may conform to the following: • ISO 9660 Level 3, which have no length restrictions for file and directory names, character sets or the number of levels in the directory structure • Joliet (Microsoft's extended ISO 9660 specification)	
K5.35	It must be possible to link the exported documents to other data exported from the system.	O2

Special comment on K5.34:

The restrictions of ISO 9660 Level 1 with regard to character set and the length of directory and file names (maximum 8 characters) are in practice bound to force through machine-generated names containing combinations of numbers. ISO 9660 Level 3 may be used if this is problematical or undesirable. However, ISO 9660 Level 3 is rarely used. To escape the restrictions of Level 1, people often resort to platform-specific extensions of ISO 9660 such as "Rock Ridge", "CD-XA" or Apple's "HFS". These are not compatible with ISO 9660 and are therefore not authorized as logical file structures for Noark transfer to a depot institution.

However, Joliet, Microsoft's extension to ISO 9660 Level 1, is of a different character, since it uses two parallell filenames for each file and directory: an 8-character name conforming to the specifications of ISO 9660 Level 1, and a Joliet-specific name with up to 64 characters based on a Unicode character set (ISO 10646). Only Windows 95/98 and Windows NT 4.0/5.0 systems currently have access to "long" Joliet filenames, but all other ISO 9660-compatible systems will see Joliet's "short" filenames - and only these. Other systems will simply ignore Joliet's file system no. 2.

Pending the new ISO standard which will replace ISO 9660, Joliet may be accepted as a file-structure format for Noark transfers.

5.5 Procedure requirements

The introduction of electronic document storage instead of paper-based records will require major changes in daily routines for both registry personnel and executive officers. Many procedures must be changed, and careful planning is required before the new system is implemented. Many tasks which currently require a lot of time, will disappear. This applies, among other things, to all work relating to physical filing, retrieval, shelving, distribution and lending-out of cases and documents to executive officers and managers. In addition, new tasks seem to belong naturally to the registry. This means different qualifications are required from registry personnel.

The registry must be responsible for controlling the quality of the electronic records, for instance by checking that the correct document is linked to the correct version in Noark. The registry should be responsible for handling the official e-mailbox of the organization. All scanning of incoming documents should also be assigned to the registry. This also applies to converting into archival format, even if it is possible to let executive officers do this directly.

Even IT personnel will feel the effects strongly. They will be responsible for making sure the electronic records are in order at any time, and for the security in terms of daily backup, etc.

5.5.1 What archive formats should be selected?

The organizations must make a choice in terms of which of the four formats should be used for long-term storage of electronic documents. It is possible to use a mixture of formats. Incoming scanned documents may, for instance, be stored in TIFF format, some e-mail may be stored in ISO Latin-1, outgoing documens may be produced directly in SGML or converted from a word processor format into PDF. Alternatively, one may choose to store everything in one format only. In that case, the options left will be PDF and TIFF, since graphics (scanned documents) cannot be converted into the other formats. Standardization in terms of using only one format has its advantages. Converting batches of documents into other formats will, for instance, be much simpler.

5.5.2 Gradual implementation of electronic recordkeeping

It is possible to implement electronic recordkeeping gradually. For many, the easiest thing is to start by storing outgoing documents electronically. Many already do this today, using systems based on Noark-3.

A situation with a mixture of electronic and paper-based documents normally requires that all main documents within a case are stored either electronically or on paper. Unless all main documents within a case are electronic (e.g., only the outgoing documents are), the electronic documents of the case are merely to be regarded as work copies - not archival copies. In such a situation, all documents which have been created electronically, must be printed on paper, and these printouts must be stored in traditional records together with the original paper documents. During transfer to archival repository, the paper-based records

should be transferred. The electronic documents may be transferred in addition if this is desirable.

Noark permits *attachments* to be stored on paper even for electronically stored cases (see requirement K5.11). It may, for instance, be deemed inappropriate to scan such attachments as thick reports and comprehensive technical sketches; these may be stored in paper form. According to Noark, a case may still be regarded as electronic if the front page of the *main document* is scanned or a reference document is used as main document and the entire document is stored on paper (see paragraph 5.2.3 and requirement K5.12).

The requirement that all main documents be stored electronically for the case as such to be ragerded as electronical (possibly by scanning parts of the main document) means, in practice, that consistently electronical filing requires extensive *scanning* of incoming paper documents, at least of incoming main documents.

If there is a mixture of electronic and paper-based cases, they belong naturally to separate *records sections*.

5.5.3 Procedures regarding filing of documents

- *Incoming paper documents:* Most documents received by the organization will for many years still be paper documents sent as mail. Incoming paper documents must first be scanned in order to be stored electronically. During scanning, an electronic snapshot of the document is taken, and this snapshot is saved in a raster graphics format. One may decide what format to use. If TIFF is selected as archival format, the natural thing would be to transfer the document directly to this format. During scanning, one may also select picture quality - e.g., resolution. The highter the resolution, the more space is required for the document. Quality must thus be weighted against space requirements.

  The organization must decide who is responsible for the scanning of paper documents. The scanned documents are to be linked to registry entries and cases in the Noark system. It therefore seems natural that the registry should be responsible for the task of scanning documents.

- *Incoming e-mail:* Electronic document exchange is more and more used, and public organizations have already started exchanging official documents using e-mail. Procedures regarding e-mail are described in more detail in chapter 10, which also describes how information from the Noark system of the sender may be exchanged as a separate attachment ("Noark head"). This information may go straight into the system of the addressee while at the same time the transferred document is associated with the pertinent registry entry and case.

  The organization should maintain an official e-mailbox, and the task of handling this should be assigned to the registry. If e-mail is sent straight to the executive officers, they should follow the procedures described in chapter 6.

  Incoming e-mail may enter the electronic records directly as soon as they have been associated with the pertinent case. If an exchange format has been used that is identical to the archival format of the organization, no conversion is necessary.

- *Internally produced documents:* The vast majority of outgoing documents will be produced by executive officers using text editors. The same applies to internal documents. Executive officers will normally make sure the documents are associated

with the pertinent case and registry entry. However, it is necessary that the registry carry out subsequent quality control. The document production should be as closely integrated with the registry system as possible, so that. for instance, information from the case and registry entry can be easily merged straight into the document - or vice versa. What executive officers are permitted to do at any stage of the process, is described in chapter 6. It is possible to formulate procedures where the executive officers themselves convert documents into archival format, but even so, the registry needs to carry out quality control.

5.5.4 Converting into archival format

The conversion into archival format may be carried out at different times. It is recommended to do it as soon as possible after the document has been received (incoming documents) or produced (outgoing and internal documents). However, it should be possible to convert several documents in one operation (batch job) at a later stage.

When a document is converted into archival format, the production format may be deleted, unless regulations require that both formats be preserved.

5.6 Essential tables in the module

Only essential tables are included here. For a complete overview of the tables in this module and their attributes, see part II, Technical specifications, chapter 14.

Table name	Text
Document link	Establishes a relationship between the registry entry and the case document (document description). Also contains information on the type of document (main document, attachment, etc.) and the sequence of the documents within the registry entry. See also paragraph 14.3.
Document link meeting document	Establishes relationships between a meeting document and the individual documents which are included here. Also contains information on the type of document that is involved (draft, minutes, etc.) and the sequence of the documents within the meeting document. See also paragraph 14.6.
Document description	Contains information on the case document, such as category (letter, report, circular, etc.) and title (heading). Also refers to the physical location if the document is stored on paper. The attribute *Document status* indicates how far the document has come in its life cycle. The tables also contain attributes for managing the access to the documents (*Access code*, *Access group*, *Authority*, *Date of downgrading*, *Downgrading code*). See also paragraph 14.3.
Version	Contains information on the specific version of the document, as well as what versions and formats the document has been stored in (”variant” is used technically to embrace both these categories). The most common formats are production format and archival format. The pertinent version variants are: a publically available version of

Table name	Text
	the document and a digitally signed version, for instance in PEM form (Personal Enhanced Message). See also paragraph 14.3.
Topic word	Contains topic (subect) words and keywords for the specific document. See also paragraph 14.3.
Note	Contains notes on a case, a registry entry or a version of a case document. This table is also described in connection with the records management module. See also paragraph 14.2.
Additional information	Contains various kinds of additional information on a case, a registry entry or a version of a case document. This table is also described in connection with the records management module. See also paragraph 14.2.
Digital signature	Contains one or more digital signatures (stored in binary form) and is linked with versions of documents. Digital signatures may be used to guarantee the authenticity and integrity of e-mail and filed case documents. Information on the verification itself is also stored here. See also paragraph 14.3.

5.7 Changes from Noark-3 and Koark

In Noark-3 and Koark, electronic recordkeeping is for all practical purposes treated at a general level. Most of the specifications in this chapter must therefore be regarded as new. Still, the following differences in detailed specifications should be noted:

- In Noark-3 and Koark, the relationship between registry entry and electronic document is 1:1. In Noark-4, it is M:M.
- Noark-3 and Koark require that the serial number should refer to electronic documents. In Noark-4, the structure of the document reference is left to the system developer.

6. PROCESS MANAGEMENT AND DOCUMENT HANDLING

Document handling in Noark-4 is associated with the records management module, which keeps track of and manages the access to the case documents, and the module for electronic recordkeeping, which handles electronic documents storage. Chapters 4 and 5 specify requirements regarding the functionality and information content of these modules.

However, the handling of case documents in an organization must also be regarded as a process. Such a handling process typically starts off when the organization receives an inquiry (a letter) from an external source, and is finished when reply is given in the form of a letter of which a copy is filed. The process may, however, be initiated internally and result in an outgoing dispatch, or it may be an entirely internal affair where all documents are internal.

The handling process includes both recordkeeping functions and case handling. The recordkeeping functions are to be managed in Noark-4, and they should preferably be part of a close interaction with functions in an associated or integrated system for case handling according to the specifications of SGK. This chapter specifies Noark's process management during document handling, including requirements regarding functionality, the relationship between the different process stages and the rights and restrictions of the various participants. Furthermore, the process management of Noark is placed in a context spanning the entire process, which also includes the functions of an external or integrated case handling system.

First, however, it is necessary to describe and specify the handling process as such. This chapter describes the handling process of the administrative work flow. For work flow which also includes political bodies and other kinds of boards, councils and committees, see chapter 9, which specifies functionality for board handling.

6.1 The handling process: work flow and document flow

The handling process of administrative work flow may, from a recordkeeping point of view, be divided into the following three process courses:

1) Incoming documents: reception, registration, distribution and filing
2) Case handling (processing), including the production and storage of case documents
3) Internally produced documents: registration, dispatch (external or internal) and filing

If the case handling is due to an incoming document, the work flow includes all three process courses. If it is due to an internal initiative, it only includes the last two.

The three process courses occur primarily in this sequence, but some functions may be performed in parallel. This applies to things like the filing of incoming documents, which may occur at the end of the whole process, as well as the production and registration of documents (courses 2 and 3).

Process courses 1 and 3 primarily include recordkeeping functions, but there is some interaction between the registry office and the case handling (managers, executive officers). Process course 2 primarily includes case handling functions, but there is also a recordkeeping function associated with the filing of case documents. All three process courses therefore require certain management functions in Noark, preferably closely integrated with work flow functions in an associated case handling system.

In addition to the document-related handling process described here, one essential recordkeeping function is to keep track of the individual cases to which the documents belong, and of how the handling process develops at case level. Noark therefore also contains certain control mechanisms for the handling process at case level.

Following is a description of the most common procedures regarding the various handling courses. Document production and the handling of internally produced documents (courses 2 and 3) are treated together because they are normally tightly interwoven. A separate paragraph, 6.1.3, gives a more detailed description of procedures and functions relating to electronic case handling and document flow, as they may be defined in an integrated interaction between Noark and an associated case handling system.

6.1.1 Handling incoming documents

Incoming documents are case documents which the organization receives from some external organization. In Noark, these are registered as document type I.

If the recordkeeping and internal document flow is *paper-based*, Noark-4 should support the following procedures:

1a) Centralized mail reception receives paper documents as mail or fax.

- Registry office stamps, applies filing plan code and registers in Noark as well as produces mailing list or daily registry.
- Registry office distributes to case distributor (manager) or straight to executive officer, possibly accompanied by mailing list to manager.
- Any case distributor (manager) distributes to executive officer; distribution is registered in Noark directly or via feedback to the registry office.
- Manager informs registry office about what is to be exempt from public access and, possibly, registers this directly in Noark.
- Registry office presents public register (electronic export or paper printout).
- Depreciation of registry entry in Noark as well as filing are carried out as documents return to the registry office after processing, together with any outgoing replies.

1b) Executive officer receives case document on paper straight from sender, as mail or fax.

- Executive officer forwards document to registry office; then: as 1a.

1c) Centralized mail reception receives documents as e-mail or datafax.

- If documents are considered case documents, they are printed on paper; then: as 1a.

1d) Executive officer receives case document as e-mail or datafax straight from sender.

- Executive officer forwards document to registry office; then: as 1c.
  Alternatively:
- Executive officer registers (temporarily) the document in Noark and forwards it to the registry office; then: as 1c.

If the recordkeeping and internal document flow is *electronic*, integrated with or in an electronic case handling system (cfr. SGK), Noark-4 must support the following procedures (see also 6.1.3, which gives a more detailed description of electronic work flow and document flow):

1e) Centralized mail reception receives documents as e-mail or datafax.

- Registry office registers in Noark, checks any automated registration effectuated on the basis the Noark "head" (see ch. 10) and immediately files documents in electronic records.
- Registry office distributes electronically to case distributor (manager) or straight to executive officer.
- Any case distributor (manager) distributes to executive officer; distribution is registered in Noark.
- Manager temporarily suspends block of public access in Noark and, if appropriate, applies access code.
- Registry office presents public register (electronic export or paper printout).

As a rule of thumb, it is assumed that all case handling and management functions are carried out from the parties' normal user environment in the case handling system.

1f) Executive officer receives case documents as e-mail or datafax straight from sender.

- Executive officer forwards document to registry office; then: as 1e.
  Alternatively:
- Executive officer temporarily registers in Noark and files document or forwards to registry office for filing.
- Case handling (processing) may start immediately or be delayed until distribution procedure is completed as in 1e; then: as 1e.

1g) Centralized mail reception receives documents on paper, as mail or fax.

- Document is scanned, registered in Noark and filed electronically.
- The original is filed or disposed of, depending on whether paper-based or electronic version is archival copy; then: as 1e.

1h) Executive officer receives case document on paper straight from sender, as mail or fax.

- Document is forwarded to registry office; then: as 1g.

In principle, combinations of the above procedures are possible. For instance, the executive officer may register received documents even if the recordkeeping is paper-based, or the document flow may be electronic while filing is carried out on paper. However, this would

not pose any further functional requirements in Noark beyond what follows from the above procedures.

6.1.2 Handling internally produced documents

Internally produced documents are the results of internal processing of some kind - letters, memos, reports, drafts, etc. In Noark, they are registered as being of document type U, N, X or S.

If the recordkeeping and document flow is *paper-based*, Noark-4 should support the following procedures:

2a) Executive officer or manager registers, finalizes and dispatches case document.

- (If new case:) Executive officer reserves new case in Noark.
- Executive officer reserves (temporarily registers) the first available registry entry of the case.
- Document is finalized in paper printout and with the required copies, etc. (by executive officer and, if appropriate, one or more managers and, possibly, typist service).
- Document is dispatched (by executive officer, manager or separate service).
- Executive officer/manager may depreciate incoming document.
- File, including copies, any drafts to be filed and any previous documents in the case are forwarded to the registry office for filing.
- The registry office checks and, if appropriate, finalizes the registration in Noark, possibly depreciates the registry entry for incoming document and files the documents.

2b) Executive officer finalizes document draft and forwards it to others for final processing and dispatch.

- Executive officer finalizes draft on paper and, possibly, in a word processor file which is available to others involved in the process.
- Any manager(s) add corrections to the draft.
- Finalized draft forwarded to anteroom or similar, which
  - (if new case) reserves new case in Noark or inquires registry to reserve new case
  - (if registry entry is to be applied to document as reference) reserves (temporarily registers) first available registry entry in case
  - finalizes document
- Document is sent for signing and dispatched (by executive officer, manager or separate unit).
- File, including copies, any drafts to be filed and any previous documents in the case, are forwarded to the registry office for filing.
- The registry office registers in Noark or checks and, if appropriate, finalizes the registration effectuated, possibly depreciates the registry entry for incoming document and files the documents.

There may also be procedures which are somewhere between 2a and 2b, e.g., drafts which have been processed by the manager may be returned to the executive officer for finalization, or the manager himself may finalize the document. However, this would not pose any further functional requirements in Noark beyond what follows from 2a and 2b.

If the recordkeeping and internal document flow is *electronic*, integrated with or in an electronic case handling system (cfr. SGK), Noark-4 should support the following procedure:

2c) Executive officer and/or manager registers and finalizes document in electronic form and dispatches it via e-mail or on paper (mail, fax)

- (If new case:) Executive officer reserves new case in Noark
- Executive officer reserves (temporarily registers) first available registry entry in the case and associates the document(s) with it.
- Document(s) is (are) finalized electronically (by executive officer and, if appropriate, one or more managers).
- Document(s) is (are) dispatched electronically or in paper printout (by executive officer, manager or separate unit).
- Executive officer/manager depreciates any incoming document.
- The finalized electronic edition(s) of the document(s) is (are) forwarded to the registry office for checking and filing.
- The registry office checks and, if appropriate, finalizes the registration in Noark, including any depreciation of the registry entry for incoming document, and files the document(s).

2d) The executive officer and/or manager produces document in an external production system (case handling system or word processor), whether or not integrated with the Noark system, and transfers it to the Noark system for registration, dispatch and filing.

- The executive officer/manager finalizes the document in the production system; then: as 2c.

As a rule of thumb, it is assumed that all case handling and management functions are carried out from the parties' normal user environment in the case handling system. A more detailed description of electronic work flow and document flow is given in the next paragraph.

6.1.3 Electronic work flow and document flow

Electronic work flow and internal document flow may improve the efficiency of an organization considerably. At the same time, such a handling process requires that work procedures be modified considerably compared to what is common practice today. The following gives a more detailed description of how such a handling process may be prepared. The emphasis is on recordkeeping and case handling procedures, and it is assumed that the functionality of Noark-4, integrated with or in a case handling system, is exploited.

Mail reception
Incoming documents are received, preferably in a centralized mail reception, but some are likely to be sent straight to the executive officers. The following procedures must be enforced during the reception phase (the sequence may vary slightly, depending on how the recordkeeping and case handling systems are designed):

- Documents are registered/entered into records (records management module of Noark) either by the registry office or by the executive officer with subsequent control by the registry office. If documents are received by e-mail from an organization that uses

Noark, parts of the registration may be carried out automatically if a Noark "head" is used (see ch. 10).

- If the documents are received in paper form (mail, fax), they must be transferred to electronic form by scanning. This operation should always be carried out by the registry office. The documents may be processed into text form by OCR software, but the OCR version is to be considered an adapted version and cannot be used as archival copy (see below regarding OCR as a tool for executive officers).

- The documents are filed electronically in an approved archival format, cfr. ch. 5. If the recordkeeping is electronic, any originals in paper form may be disposed of, or they may be filed as a kind of backup measure. The processing is based on the electronic version of the document, which is considered the archival copy.

Distribution and presentation of public register
Distribution of incoming documents for processing involves registering the administrative unit and, possibly, the executive officer in Noark. If the executive officer is registered, responsibility for case handling (processing) is assigned to him or her. If only the administrative unit is registered, the responsibility for case handling is assigned to the manager of the unit. The subsequent procedure should be approximately as follows:

- Managers and executive officers should automatically be presented with a summary of new cases for processing (i.e., received documents). This may be effectuated through a case handling system or by other means integrated with the recordkeeping system. If no such means are available, managers and executive officers should be able to search for their cases in a simple way from their normal user environments.

- Documents which have been assigned to a manager (or possibly a designated case distributor), are further distributed to the executive officer. This is effectuated by registering the executive officer. The rest of the procedure is as in the previous indent.

- If the organization is temporarily exempting documents from public access (see paragraph 8.2.2.4), the person responsible for the initial case handling (normally the manager) should decide whether the document and/or registered information should be exempt from public access. Once a decision has been made, the blocking code (access code XX) in the recordkeeping system is suspended and access code and, if appropriate, access group are registered in cases where information is to be screened.

- The registry office presents public register for documents whose temporary blocking has been suspended, cfr. paragraph 8.2.2.5.

Case handling and document production
Once an executive officer has received a document for processing, the case handling itself is sparked off, comprising of case preparation, evaluation and decision as well as document production. Alternatively, the case handling (processing) may be initiated on the basis of an internal initiative. The processing as such is outside the scope of the registry and should not be handled by Noark. However, some tasks relating to document production concern the recordkeeping function and thus Noark. Noark-4 should be designed to maintain these functions in a way that fits in with a rational handling process. It is therefore necessary to describe this process in order to maintain such tasks in Noark.

The following procedures and functions should be maintained:

- As part of the case preparation, an executive officer should be able to retrieve documents and other information from the records and other internal and external electronic sources of information. This should preferably be effectuated from the same user environment, cfr. the description of the interaction between Noark and SGK in paragraph 2.2.2, figure 2-1.

- To be able to reuse parts of documents which have been scanned (stored in TIFF or similar format), the executive officer should have access to an OCR tool which transforms (parts of) the document into a format which may be edited. This tool should be integrated with the case handling system but does not concern Noark (even if the documents which are processed, will often be retrieved from electronic records).

- The document production may take place entirely outside of or more or less integrated with Noark. If the document being produced is known to be a case document which is to be registered in the recordkeeping system, using the link with Noark in the document production, in accordance with the principles described in the following, will normally be rational and improve the quality. This maintains rational transfer of information between registry and document, correct linking in the registry and secure depreciation linking between document and reply document.

- When the executive officer is producing a new document, he associates it with the first available registry entry in the case he is working with, or he may ask for the first available case number in order to create a new case. Both should be attainable through the use of simple commands from his normal user environment, and should result in automated registration in the recordkeeping system.

- The executive officer registers the necessary registry information, such as addressee, title and references. For reply letters, a temporary depreciation link is established with the received document (formal depreciation is carried out later), and most of the registration may be automated by transferring information from this. In the production system (case handling system or word processor), the executive officer retrieves a document template for the category of document he wishes to produce, and relevant information is automatically transferred from the recordkeeping system: addressee, title, references, etc. The document templates should be designed so as to address the need to transfer relevant information between the records management of Noark and the document.

- The executive officer should be able to decide who is to have access to the document as long as he is producing it. Still, the person responsible for the case (if different from the executive officer) as well as the manager(s) of the concerned administrative unit should have access to the document in special circumstances, e.g., if the executive officer is away, if he has quit his job, etc. Apart from this, read and write access to the document is reserved for the executive officer and any person to whom he has explicitly granted access. Only when the executive officer has finalized a draft or finalized the document for dispatch should it be available to others.

- The executive officer and his/her manager(s) should be able to produce and file an arbitrary number of versions. From a recordkeeping point of view may be envisaged the following alternative procedures, which Noark should be able to handle:

- After the initial linking up with the recordkeeping system as described above, document production proceeds in the document production system with Noark knowing only that a document is being produced. During production or after the document has been

finalized, it should be stored in Noark in one or more versions, and the registry information should be updated accordingly. Versions stored in Noark may not be modified. When the document has been completed in its final version, it is dispatched, and finishing recordkeeping functions are carried out as described below.

- The executive officer prepares a document, finalizes it and files it in Noark. If the document is finalized, i.e., the manager does not need to check or process it further, it is immediately sent off for dispatch and finalizing recordkeeping functions. If the document is a draft which some manager(s) is (are) to process further, it constitutes the initial version of the document and is thus filed in permanent form. The same procedure may be repeated at several stages, for instance from the section manager to the department manager and from the department manager to the director general. After the last person has finalized the document, it is sent off for dispatch and finalizing recordkeeping functions.

- The executive officer and any manager(s) or other involved party prepares a document which is finalized in only one version. The document is available from Noark during the whole process, with the restrictions indicated above. When the document is finalized, it is filed permanently and sent off for dispatch and finalizing recordkeeping functions.

Finalization, dispatch and finalizing recordkeeping functions
When a document is completed in its final version, the person who finalizes the processing (executive officer or manager) indicates that the document is finalized. This is a go-ahead signal for dispatch and finalizing recordkeeping functions. Parts of these functions should be carried out by the executive officer or manager, the rest by the registry office. The registry office is also responsible for quality control of recordkeeping functions carried out by the executive officer or manager. The following procedures are involved:

- Dispatch may be effectuated electronically (via internal or external e-mail), via fax or on paper (traditional mail). Electronic dispatch should preferably take place in an e-mail system which is integrated with the recordkeeping system, but may also be carried out in a separate system, cfr. ch. 10. The dispatch should be carried out by the manager/executive officer or by the registry office. Unless the checking may be carried out by the system, the person who carries out the dispatch must make sure the dispatched copy is identical to the archival copy. It is also worth considering the need to check that an electronic dispatch reaches the addressee in readable and unaltered form.

- For all filed versions of a document, the system should automatically register who has carried out the filing. This makes it possible to check that the final version of the document originates from the executive officer/manager indicated in the document. If further security is needed for the authenticity of documents during internal processing, digital signatures may be used (see ch. 10).

- The executive officer should be able to depreciate one or more received documents using automated functions when a reply document is dispatched. In such a case, the system should include functionality for handling a situation where some organizations require the authorization of a manager for the depreciation to be valid. If neither manager nor executive officer carries out depreciation, the registry office is responsible for it.

- It will usually be necessary, or at least appropriate, to evaluate the necessity of public access when a document is finalized and dispatched. The executive officer and/or

manager should be able to suspend any temporary blocking and register any access codes for documents which are finalized, including registry and case information.

- After finalization and dispatch, the document (final version) should be stored in archival format. This task is best assigned to the registry office. However, it should also be possible for the executive officer or manager to do this, especially in those cases where they dispatch documents electronically and the exchange format is identical to the archival format.
- The registry office performs the necessary checks on registry information and finalizes the registration.

6.1.4 Communication via the Internet (web pages)

There are cases where a public body communicates with other organizations through web pages on the Internet. For instance, a letter and attachments may be published on a web page and comments invited. The organizations may be able to add their comments directly to the web page. In such cases, the web page replaces the documents which would normally have been sent to the organization(s) and registered and filed there.

This kind of communication is problematic from a legal, recordkeeping and practical point of view. It raises important questions, such as: How does one define archival documents in this context, and where does one file them? How is this communication to be entered into records, and how is it to be guaranteed that the communication is presented in the public register in accordance with the regulations? These are questions which must be evaluated by the National Archivist and other relevant authorities, taking into account the Archives Act and the Freedom of Information Act, etc.

Noark-4 is not trying to prescribe specific solutions for this kind of communication. It is not the task of Noark to illuminate the professional and legal problems raised by this kind of communication. However, it is assumed that solutions can and should be found within the framework of registration and electronic recordkeeping specified by Noark-4.

It is emphasized that the communication via web pages that is described here, should not be confused with »ordinary» information published on web pages. Information retrieved from the Internet in connection with case handling (processing) is not considered records material unless it is part of a case in a way that ought to be documented. The reader is referred to the discussions on records weeding in paragraph 2.1.2 and SGK document storage in paragraph 2.2.2.

6.2 The process management functions of Noark

Noark systems should have mechanisms for controlling *what recordkeeping functions* may be performed *when* and *by whom* during the different phases of the handling process. This kind of process management should form the basis of the more sophisticated *quality control* functions which are required when executive officers are allowed to perform certain defined registration and updating functions themselves. It is assumed that the process management will interact with detailed access management, centralized subsequent control of registrations and automated logging of effectuated changes in defined areas.

The starting point of the process management is the various recordkeeping functions (the activities during registration and filing), subdivided into defined process phases. Each phase is associated with one or more alternative status values. Each status value is associated with rules which define what functions should be available and what restrictions should apply for the various parties involved at the process stage in question. The rules also specify conditions which must be satisfied for a status value to be modified, and thus for the process to move on to the next stage.

The process management is associated with three main categories of parties involved: the *registry office* (archives, archivists), *executive officers* and *managers*. This chapter describes the parties' specific registration rights at the various process stages. For further details on user rights, see chapter 8.

The process management of Noark-4 is associated with the status attributes in the tables *Case*, *Registry entry* and *Document description*.

K6.1	Rights regarding the registration of case information should be managed through values in the attribute *Case status* in the table *Case*.	O
K6.2	Rights regarding the registration (entry into records) of incoming and internally produced documents should be managed through values in the attribute *Registry status* in the table *Registry entry.*	O
K6.3	It should be possible to configure the system so that the process management is not used for one or more registry management units, or for the entire base. This should lead to the attribute *Registry status* automatically being assigned the value **J** when the registry entry is created. In an enhanced version (requirement type O1), it should nevertheless be possible to change the value to **A** according to the rules described in this chapter. Rights regarding registering information in the registry entry are managed through the values in *Registry status* in the usual manner (see K6.2).	O
K6.4	Rights regarding electronic document production and filing should be managed through values in the attribute *Document status* in the table *Document description.*	O2
K6.5	If Noark is integrated in or with an electronic case handling system (cfr. SGK) or a similar system, then: • It should be possible to modify values in *Case status*, *Registry status* and *Document status* using automated functions in Noark, effectuated when the user issues commands or defines status values, etc., in the case handling system.	S

	• Values in *Case status*, *Registry status* and *Document status* should manage user rights in Noark even when Noark functions are accessed from the case handling system.	

Otherwise, the process management is based on the following principles:

- The next process stage is entered into by changing a status value. Defined activities must be completed (and registered) for the system to accept a change to the next status value. This control function should ensure the complete execution of the registration task.
- For executive officers and managers, a change of status code should at the same time block any activities relating to previous process phases. The registry office should have registration access during most process phases, even for registering on behalf of the executive officer or manager. For some process phases, however, it is assumed that the registration access of the registry office is limited to special purposes, such as correcting errors. The registry office should not be able to change the contents of *documents* or *notes* created by executive officers or managers.
- The status code is modified when the activities relating to a proces stage are completed. The modified status value will then be a signal - usually to some other involved party - to perform follow-up activities. It is up to the individual vendors to add functions for alerting various parties and providing summaries of tasks for which they have follow-up responsibilities.
- When the entire process has a status that signifies "finished", registration opportunities should generally be blocked. These blocking mechanisms should prevent unauthorized or inadvertent modification of registered information. There should nevertheless be options for defining the status of the previous stage in order to correct errors, tackle unexpected circumstances, etc. Such options are normally reserved for the registry office.

The system should offer alternative status values at the different process stages to make it possible to choose between *alternative process courses* during registration. This should adapt the system to a variety of uses. The process management includes status values adapted to traditional, centralized registration and paper-based recordkeeping as well as to electronic case handling where executive officers and managers themselves perform registration tasks. The system must, furthermore, make it possible to combine different uses, so that alternative process courses may run in *parallel* within the same organization. Such a combination of uses will be in demand as long as electronic and paper-based recordkeeping are carried out side by side. The options are also necessary for it to be possible to adapt the system in a flexible way to a diversity of organizations and procedures as well as the widely diverse levels of competence in the user organizations

The process management functions are detailed based on the figures below. Status values are associated with the individual process phases as "flags". In each status value, all previous codes in the sequence will be logically incorporated. The value **A** thus indicates that all previous activities in the process have been completed.

The process management has a flexible design with regard to the distribution of roles between managers and executive officers. It does not include status values for managers' authorizations of registrations, but leaves the more detailed handling of the manager/ executive officer relationship to a surrounding case handling system.

It should be possible to perform all registration tasks which managers or executive officers carry out, within their normal user environments, i.e., in an associated or surrounding case handling system. In such a case, it must be possible to update the Noark status values on the basis of registrations carried out in the case handling system. However, unless Noark is part of an integrated interaction with a case handling system, the registrations of the executive officers and managers must be carried out directly in the Noark system.

6.2.1 Process management for cases and case information

New cases are created in Noark when documents which constitute a case are received or produced, i.e., documents which address a new question for processing, cfr. 4.2.1 above. A case must be created before the associated documents (registry entries) may be registered, and the case must permit new registrations to be carried out. When a case is finalized, it should be blocked to any kind of registration and updating of both case information and associated registry entries and documents.

The process management is associated with the following values in the attribute *Case status:*

R = Reserved by executive officer (or by the registry office or a manager on behalf of the executive officer)
B = Being processed
A = Finalized
X = Case exempt from process management
U = Case dismissed

The value R is assigned when the executive officer (or other person on behalf of the executive officer) reserves a new case in order to register a self-produced or incoming document. When the registry office registers a new case or updates the registrations of a reserved case, the value B is assigned. The value A is assigned when all new registration and updating in or regarding the case should be completed, for instance in connection with periodic completion.

If more detailed process management is desired, for instance in connection with board handling (see chapter 9), the value B may be replaced with customized values. In such a case, different characters from the ones predefined above must be used.

If process management through case status is not desired, the value X may be used as a default value and all cases assigned this valued. Alternatively, R may be used for reservations by the executive officer and X as a fixed value when the registry office has registered or updated something.

Functional requirements regarding case status:

AR = *Registry office["Arkiv"]*. Rights and responsibilities may apply to the entire base or be limited to the concerned registry management unit, depending on the roles of the party involved (see chapter 8).

LD = *Manager ["Leder"]*. Rights and responsibilities are limited to the person's administrative unit, cfr. ch. 8. (Note that when a person who is a manager fills the role as executive officer, he is indicated by SB in the table below, cfr. ch. 8).

SB = *Executive officer ["Saksbehandler"]*. Rights and responsibilities are limited to cases where he or she is case responsible, or registry entries for which he or she is executive officer. Responsibility is limited to cases for which he or she is case responsible. See also chapter 8.

When AR, LD or SB is in brackets, it means that they should be assigned the right concerned in the system, but that it is only meant to be used in special circumstances, e.g., in order to correct errors or when the party originally vested with the rights cannot perform the task himself.

Re-quire-ment no.	**Status value**	**1) Status value set by: 2) Condition for setting value:**	**Follow-up responsibility assigned to**	**Right to register**	**Right to modify status**	**Type of re-quire ment**
K6.6	R	1) SB, (AR), (LD). 2) Executive officer registered automatically or manually.	AR	AR, SB, (LD)	AR	O
K6.7	B	1) AR. 2) Set automatically as AR creates case or updates case with status R.	AR	AR: generally. SB, LD: attributes according to ch. 8.	AR	O
K6.8	A	1) AR. 2) Presupposes that all associated registry entries have *Registry status* J or A (for systems which have this attribute). If the case is stored electronically, registry status is assumed to be A.	None	AR, LD, SB: attributes according to ch. 8.	AR	O
K6.9	X	1) AR. 2) Set automatically as an alternative to B when X is defined as default value.	AR	AR: generally. SB, LD: attributes according to ch. 8.	AR	O
K6.10	U	1) AR	None.	None	AR	O

K6.11	When SB reserves a new case, he should automatically be designated case responsible, and he should not himself be able to modify these values. AR and LD for the concerned administrative unit should be able to modify the values.	O
K6.12	It should be possible to replace the value **B** in *Case status* with customized values, configured in the system. The letters R, B, A, X and U may not be used for such values.	A

6.2.2 Process management for registering incoming documents

Incoming documents (document type I) are registered (entered into records; records management module) and then distributed for processing (case handling). When the processing has been completed, the document returns to the registry office for finalizing registration, including depreciation if not carried out by executive officer. Electronic documents are filed in connection with initial registration, i.e., before processing. Paper documents are filed after processing has been completed.

The recordkeeping aspect of document processing is controlled by the following registry status values:

M = Temporarily registered by the registry office
S = Initially registered *or* updated by the executive officer/manager
J = Registered *or* checked by the registry office
A = Registration finalized (by the registry) office

The following figure illustrates the process: alternative process courses, different stages, parties involved and status values.

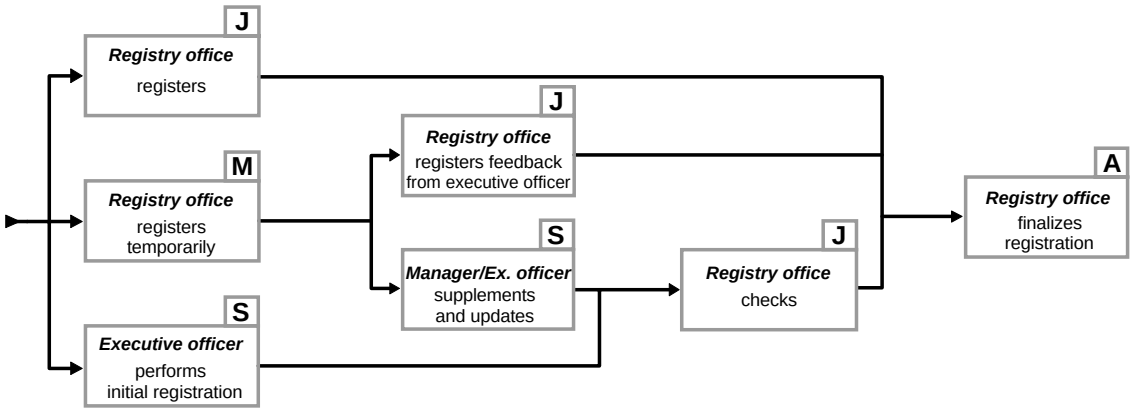


Figure 6-1: Incoming document - handling process, change of registry status

The status value **M** is used by the registry office as a signal to the manager/executive officer to update the registry entry (typically, to register the responsible executive officer). **S** is used by executive officers and managers when they themselves perform the initial registration or update what is registered in the records. When the role of the registry office is limited to checking the registrations performed by executive officers/managers, a change of status value to **J** indicates that checking has been carried out. The value **A** is used to indicate that the registration is finalized and to block any attempt to make changes.

Functional requirements regarding registry status for incoming documents:

AR = *Registry office ["Arkiv"]*. Rights and responsibilities may apply to the entire base or be limited to the concerned registry management unit, depending on the roles of the individual party, cfr. ch. 8.

LD = *Manager ["Leder"]*. Rights and responsibilities are limited to the person's administrative unit, cfr. ch. 8. (Note that when a person who is manager, acts as executive officer, his role is indicated as SB in the table below, cfr. ch. 8).

SB = *Executive officer ["Saksbehandler"]*. Rights are limited to cases for which the person is case responsible, or to registry entries for which he is executive officer. Responsibility is limited to cases for which he is case responsible. See also chapter 8.

Enclosing AR, LD or SB in brackets indicates that they are to be assigned the indicated right in the system, but that it is only meant to be used in special circumstances, such as for correcting errors or when the person who was originally assigned the right, is not able to complete the task himself.

Re-quire-ment no.:	**Status value:**	**1) Status value set by: 2) Condition for setting the value:**	**Follow-up responsibility assigned to:**	**Right to register:**	**Right to modify status:**	**Type of re-quire ment:**
K6.13	M	1) AR. 2) Status M or J set auto-matically if AR registers. It should be possible to con-figure a default value.	SB: if executive officer is registered LD: if only adm. units are registered AR: if both are absent	AR, LD, SB	AR, LD, SB	O1
K6.14	S	1) SB/LD. 2) Status S set automatically when SB or LD registers.	AR	AR, LD, SB	AR	O1
K6.15	J	1) AR. 2) In the enhanced version, status is set to M or J automatically if AR registers. It should always be possible to configure a default value. The value J is not permitted unless adm. unit is registered (the value is then set to M instead). In the basis version, the status is always set to J when AR registers.	AR	AR: generally. SB: attributes according to ch. 8.	AR	O
K6.16	A	1) AR. 2) Presupposes that the registry entry has been depreciated. *Document status* must be **F** for all electronic documents associated with the registry entry, and they must exist in an archival format if the	None	AR, LD, SB: attributes according to ch. 8	(AR)	O1

		case is to be filed electronically.				

6.2.3 Process management for registering internally produced documents

Internally produced case documents should be dispatched either externally (document type U) or internally (document types N, X and S). The document production may either follow the integrated procedure described in 6.2.4, or it may be carried out entirely independently of the recordkeeping system - e.g., as production in a normal word processor and filing on paper.

Irrespective of the production form, all documents should be entered into records (records management module of Noark). If the document production is integrated, as described below, the registration (entry into records) happens as a natural part of the production. If the production is carried out independently of the recordkeeping system, registration is normally carried out after the documents have been finalized, possibly accompanied by a temporary registration (reservation of registry entry) when the registration commences.

The recordkeeping aspect of the document handling is controlled by the following values in *Registry status:*

R = Reserved by executive officer, manager or registry office
F = Finalized by executive officer or manager and ready for dispatch
E = Dispatched by executive officer, manager or other party
J = Registered *or* checked by registry office
A = Finalized by registry office

The following figure illustrates the process: the alternative process courses, different stages, parties and status values.

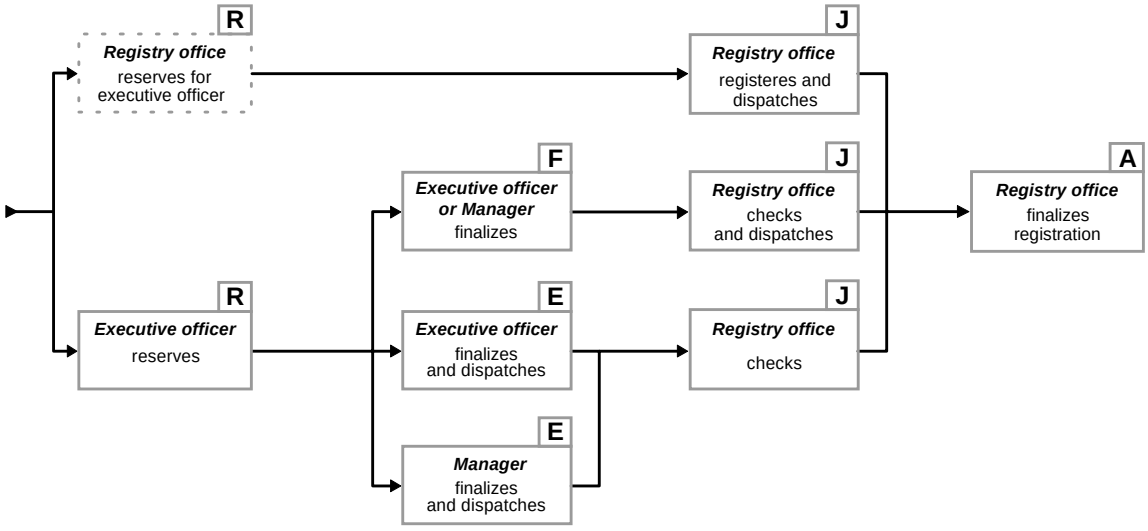


Figure 6-2: Internally produced document - handling process, change of registry status

The status value **F** is used by executive officers/managers when they do not effectuate the dispatch themselves. F is then a signal to the registry office or other party to effectuate dispatch. When executive officers/managers *both* finalize and dispatch, the value **E** is used (F is then considered as logically incorporated in E, and is not used as a step in between). When the registry office *both* registers and dispatches, the status should be set to **J** without E being used in between. In such cases, dispatch (E) is logically incorporated in J.

Functional requirements regarding registry status for internally produced documents:

AR = *Registry office ["Arkiv"]*. Rights and responsibilities may apply to the entire database or be limited to the concerned registry management unit, depending on the roles of the individual party, cfr. ch. 8.

LD = *Manager ["Leder"]*. Rights and responsibilities are limited to the person's administrative unit, cfr. ch. 8. (Note that when a person who is manager, acts as executive officer, his role is indicated as SB in the table below, cfr. ch. 8).

SB = *Executive officer ["Saksbehandler"]*. Rights are limited to cases for which the person is case responsible, or to registry entries for which he is executive officer. Responsibility is limited to cases for which he is case responsible. See also chapter 8.

Enclosing AR, LD or SB in brackets indicates that they are to be assigned the indicated right in the system, but that it is only meant to be used in special circumstances, such as for correcting errors or when the person who was originally assigned the right, is not able to complete the task himself.

Re-quire-ment no.	**Status value**	**1) Status value set by: 2) Condition for setting the value:**	**Follow-up responsibility assigned to**	**Right to register**	**Right to modify status**	**Type of re-quire ment**
K6.17	R	1) SB, (AR), (LD). 2) Executive officer registered automatically or manually.	SB	SB, (AR), (LD)	SB, (AR), (LD)	O
K6.18	F	1) SB, LD. 2) Presupposes that all electronic documents associated with the registry entry have *document status = F*.	AR	AR: gene-rally. SB, LD: attributes according to ch. 8.	AR, (SB), (LD)	O
K6.19	E	1) SB, LD. 2) As for the value F. In addition, *Dispatch date* must be filled in.	AR	AR: gene-rally. SB, LD: attributes according to ch. 8.	AR, (SB), (LD)	O1
K6.20	J	1) AR. 2) As for the value F. If the main document is electronic, then the attribute *Dispatch date* must be filled in.	AR	AR: gene-rally. SB, LD: attributes according to ch. 8.	AR	O

K6.21	A	1) AR. 2) as for the value J. All electronic documents must exist in archival format for the case to be considered electronic. If the document type is N, then the registry entry must be depreciated.	None	AR, LD, SB: attributes according to ch. 8.	(AR)	O1

K6.22	When a registry entry is created with status **R**, it should not be assigned a document number. The document number should be assigned automatically by the system when the status is changed from **R** to **F**, **E** or **J**.	O

6.2.4 Process management for electronic document production and electronic filing

The production of electronic case documents is a case handling function, as described above. This function should ideally be maintained by a case handling system, based on the specifications of SGK and closely integrated with Noark - e.g., by incorporating both types of functions within the same system. Without access to a case handling, linking the Noark system as closely as possible to a word processor might be an acceptable solution.

The filing of electronically produced documents, however, is a recordkeeping function within the domain of Noark. Noark must possess functionality for maintaining the interaction between executive officers and the registry office in connection with the filing of electronic case documents. It must be possible to carry out the filing as a natural and integrated part of the production process which includes documents in different versions and formats.

The process management of Noark-4 is thus limited to the recordkeeping functions, and it presupposes an interaction with a surrounding case handling system (or similar system). Noark should primarily keep track of the stored versions and formats, cfr. the table *Version*, and know whether a document is finalized or not, cfr. the attribute *Document status* in the table *Document description*.

An integrated solution presupposes that the table *Document description* should be shared by Noark and the case handling system. Thus, Noark imposes no restrictions with regard to the values of the attribute *Document status*. The only requirement is that the status of **F** should indicate a finalized document; otherwise, there are no restrictions. If Noark is not incorporated in an integrated solution, it is recommended that the status of **B** is used to indicate that a document is being processed and not yet finalized. This value is used in the following description to indicate »not finalized».

The following values may be used for *Document status:*

B = Being processed by executive officer. This value may be replaced by one or more other values.
F = Finalized by executive officer. Obligatory value in Noark-4.

The status of B (or similar) is set automatically when the executive officer creates a document, for instance from an associated case handling system or a word processor. When the document is completed and stored in Noark (possibly in several versions), the executive officer/manager changes the document status to F. This transfers follow-up responsibility to the registry office. The executive officer/manager may, however, on certain conditions, return the status to B if circumstances so dictate.

Functional requirements regarding document status for electronic documents:

AR = *Registry office ["Arkiv"]*. Rights and responsibilities may apply to the entire database or be limited to the concerned registry management unit, depending on the roles of the individual party, cfr. ch. 8.

LD = *Manager ["Leder"]*. Rights and responsibilities are limited to the person's administrative unit, cfr. ch. 8. (Note that when a person who is manager, acts as executive officer, his role is indicated as SB in the table below, cfr. ch. 8).

SB = *Executive officer ["Saksbehandler"]*. Rights are limited to cases for which the person is case responsible, or to registry entries for which he is executive officer. Responsibility is limited to cases for which he is case responsible. See also chapter 8.

Enclosing AR, LD or SB in brackets indicates that they are to be assigned the indicated right in the system, but that it is only meant to be used in special circumstances, such as for correcting errors or when the person who was originally assigned the right, is not able to complete the task himself.

Re-quire-ment no.	**Status value**	**1) Status value set by: 2) Condition for setting the value:**	**Follow-up responsi-bility assigned to**	**Right to register**	**Right to modify status**	**Type of re-quire ment**
K6.23	B (or other values)	1) SB 2) Executive officer registered automatically.	SB	SB, (LD), (AR)	SB, LD	O2
K6.24	F	1) SB, LD. 2) Presupposes that the document is filed in Noark (in one or more versions).	AR	AR: generally SB, LD: attributes according to ch. 8.	(AR), (SB), (LD)	O2

If the document production itself is integrated with Noark, it takes place when *document status* is B or similar, and it should be completed before status is set to F. See the description of electronic document production in 6.1.3 above.

K6.25	Internal document production should take place in a system which is integrated with Noark, preferably in an integrated case handling system (cfr. SGK), or, if this is not possible, in a standard word processor with established links to/from Noark. The integration should include functions for automated and structured transfer of information between the registry entry and the document description in Noark on the one hand and the document in the production system on the other hand.	S

K6.26	When a document is created (*document status* **B** or similar), the access code of the document should automatically be set to XX, cfr. temporary blocking of recently registered information in paragraph 8.2.3.4.	O2
K6.27	As long as a case document has not been dispatched (i.e., associated with a registry entry with *registry status* **E**, **J** or **A**), whoever is responsible for registering the document according to K6.24 should be able to »take it back» for further processing by changing the *document status* from **F** to another value. In such a case, the *registry status* should automatically be set to **R**. Filing of the document in a processed form means filing a new version, cfr. K6.30.	O2

If document production takes place in a production system which is integrated with Noark as described in K6.25, it should be possible to use the following document production procedures:

- A new document is created in Noark using a command in the production system, and the necessary information in the document description and registry entry (if new) is registered. The system sets *document status* to **B** (or other similar value), and the relevant information from the document description and registry entry is automatically transferred to the document. The production and temporary storage of the document in one or more versions takes place in the production system. If necessary, it should be possible to file one or more versions in Noark. This should take place during the production process, i.e., while the *document status* is still **B** (or similar), or after the production is completed, i.e., when *document status* is set to **F**.
- The production starts in the production system, independently of Noark, and temporary storage is carried out there. When one or more versions are to be filed in Noark, the document is created in Noark and assigned *document status* **B** or **F**, depending on whether the production process is completed or not. It should be possible to create the document in the production system (as above) and to have information automatically transferred from that system to the document description and registry entry.

If the Noark system includes electronic records, but is not integrated with a case handling system or other production system which satisfies the requirements of K6.25, adding functionality for integrated document production linked directly to the Noark system ought to be considered. This presupposes that a direct link between Noark and a word processor. The functionality should, as a minimum, include automated transfer of information between *Document description/Registry entry* and the document as well as mechanisms for indicating whether a document version is being processed or has been finalized and thus filed. Such mechanisms are not included in the technical description of Noark-4.

Noark should be able to file and guarantee the integrity of an arbitrary number of electronic versions of a case document. This applies to both documents received from an external source and internally produced documents, irrespectively of whether they have been produced in a system integrated with Noark or not.

Functional requirements regarding the filing of document versions:

K6.28	Any person who has registration rights to a registry entry (see paragraph 8.2.2), should be able to associate an arbitrary number of electronic case documents (main document and any attachments) to the registry entry and file them in an arbitrary number of versions and formats. This applies to documents received from external sources as well as internally produced documents, whether the production is integrated with or independent of Noark.	O2
K6.29	It should not be possible to file new versions of documents which have *document status* **F**.	O2
K6.30	It should not be possible to modify or edit document versions which have been filed in Noark. However, it should be possible to delete them in accordance with specific rules, cfr. K6.31-K6.33.	O2
K6.31	As long as the *document status* is different from **F**, it should be possible to delete versions of documents which have been filed in Noark, for those who filed the version or for the manager(s) of the concerned administrative unit.	O2
K6.32	For document versions which are not the last one (*Active version* in the table *Version* = 0), the person who has filed the version in question, or the manager(s) of that person's administrative unit, should be able to specify a date for the deletion of the version (in the attribute *To be kept until date*). It should be possible to set such a date as long as the *Document status* is different from **F**. It should also be possible for the organization to define a default value for this attribute, specified as a time interval from the current date, cfr. the table *Default values and other configuration information*. It should be possible for the person who is authorized to set such a date, to exceed it. When the date has been reached, the system should automatically delete the concerned document version. Alternatively, this may be effect-uated in one operation for several documents and versions, for instance once a month.	S1
K6.33	When the *Document status* is **F**, only specifically authorized persons should be able to delete document versions, cfr. ch. 8. There should be different authorizations for deleting the final version of a document and previous versions. All deletion of versions of documents which have the status **F**, should be logged.	O2

6.3 Process management as compared to SGK

The process management of Noark-4, as described in this chapter, is in the border area between recordkeeping functions and case handling functions. This is due to the need for a close and well-defined interaction between these functions for the case handling (processing) to be efficient, as well as the need for adequate quality control. The description in Noark aims at placing the recordkeeping process in its proper context, which necessitates the description of individual case handling functions. From a case handling point of view, functions and requirements have been described in SGK, where a number of cases have necessitated a similar description of recordkeeping functions for the sake of the context.

As mentioned, there are three main types of parties in the recordkeeping process: archivist, manager and executive officer. The last two are primarily associated with the case handling function, but in many organizations they will also be assigned tasks which concern the recordkeeping functions, such as registration, electronic filing and dispatch. Thus, the recordkeeping system must be able to respond to actions relating to recordkeeping carried out by managers and executive officers.

The above description often emphasizes that the tasks of managers and executive officers should preferably be performed in a case handling system which is integrated with the Noark system. This presupposes that the case handling system conforms to the SGK specifications. This integration should, among other things, guarantee the automated transfer and updating of information between the Noark and SGK functions as well as efficient information searching across functions from the locations of the different parties. The integration may be implemented by incorporating both types of functions in a common system, or by letting two systems be integrated with each other via a common interface (see ch. 17 concerning interfaces).

However, Noark-4 also provides for the maintenance of simple recordkeeping processing without integrating it with or in a complete case handling system as described in SGK. Even if this is a less satisfactory solution, it will still be possible to integrate Noark with a word processor and let all types of involved parties use the Noark process management directly.

6.4 Changes from Noark-3 and Koark

The concept of process management is not used in Noark-3 or Koark. Still, both describe, to a certain extent, processes, especially in connection with electronic document production (paragraph 10.2.1 in Noark-3 and paragraph 14.2 in Koark). However, the process management of Noark-4 is more comprehensive and implemented in a more systematic way than previously. The following changes have been made in attributes relating to process management:

Basic version (requirement type O):

- The attribute *Case status* is mainly used in the same way as in Koark. This represents an enhancement of the attribute *Case completed* in Noark-3.

Enhanced version (requirement type O1):

- The attribute *Registry status* replaces the *Document status* of Koark. The functionality has been enhanced. This attribute does not exist in Noark-3.

Electronic recordkeeping (requirement type O2):

- The attribute *Document status* in Noark-4 is new.

7. MODULE FOR ADMINISTRATIVE STRUCTURE AND RECORD STRUCTURE

7.1 Purpose of module

This module has two main purposes:

- linking cases and registry entries with the *administrative unit* responsible for the processing (case handling), and thence with the person who is executive officer or case responsible
- linking cases and registry entries with the *record structure* of the organization

The administrative structure should permit an infinite number of levels, services, departments, sections, offices, etc.

Two elements of the record structure must be described by this module:

- record-organizational units (*registry management units*)
- physical/logical units for the storage of records documents (*records* and *records sections*)

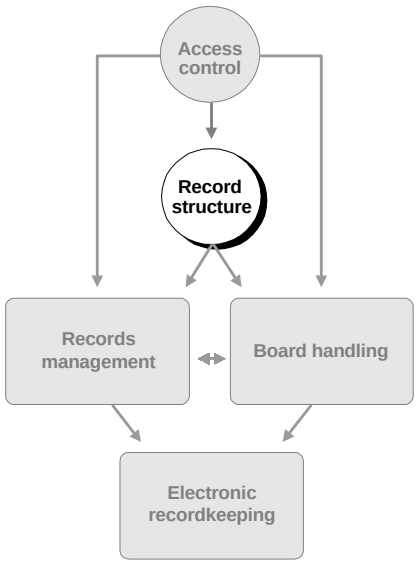


Figure 7-1: Position of record-structure module in Noark

Division into records sections is a new feature in Noark-4 and a condition for periodization of the records according to the principles outlined in chapter 12.

In this module, the administrative structure should be completely independent of the record-organizational structure. A records entity or a records section may thus cover:

- an entire administrative unit (e.g., a department)
- parts of an administrative unit
- several administrative units

The module must also allow the individual organization to operate with different kinds of decentralized registry, e.g.:

- centralized registration (entry into records) and decentralized filing
- decentralized registration (entry into records) and centralized filing
- decentralized registration (entry into records) and decentralized filing

7.2 Module design

Information on the administrative organization is handled by the table *Administrative organization.* The same table is used for all levels of the administrative hierarchy.

The most important tables for the description of the record structure are *Records*, *Records section*, *Registry management unit*, *Sorting principle* and *Order value.*

The following figure shows the relationship between these tables. For the sake of clarity, references to other tables in other modules have been included.

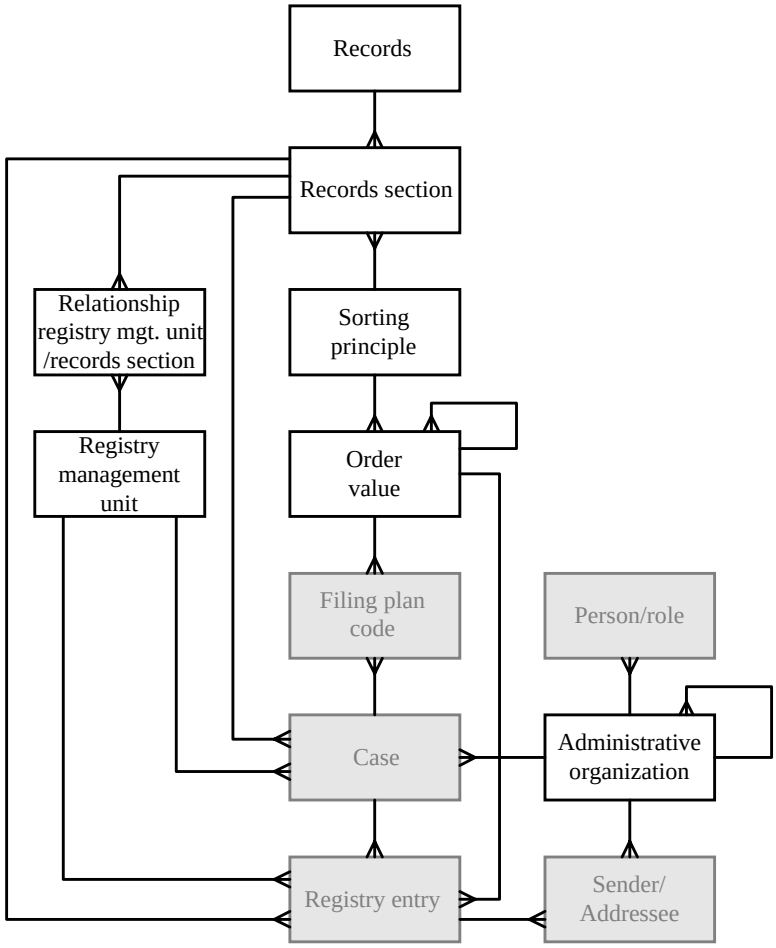


Figure 7-2: Administrative structure and record structure

7.2.1 Administrative structure

In Noark-3 and Koark, the administrative structure could only consist of two levels (usually referred to as department and office). The lowest level (office) was linked to executive officer/case responsible. This left little scope for flexibility, and large organizations, in particular, had problems describing their organization within this framework. Noark-4 must therefore permit an infinite number of administrative levels.

One way of solving this as far as the system is concerned, is by storing all data on the administrative structure in a single table, *Administrative organization*. A record in this table must contain an attribute which refers to the higher-level unit, which will be another record in the same table. On the top level, this attribute will be empty. In addition, there must also be an attribute which indicates whether the record in question is a department, an office, a section, etc.

It should be possible to preserve the organizational history by keeping shut-down units in the table. However, units which have been shut down, should not be used for registration. For instance, if a search finds a department which has been shut down, it should be able to point to the replacement department. A practical way of solving this might be to have an auxiliary table, *Alias for administrative unit*, which points from one unit to another.

K7.1	In the basic version, it should be possible to describe the administrative structure with at least three levels.	O
K7.2	In an enhanced version, it should be possible to describe an administrative structure with an infinite number of levels.	O1
K7.3	Searches for an administrative unit should automatically include any lower-level units. It should, however, be possible to perform the search without this kind of inclusion.	O1
K7.4	It should be possible to trace any changes in the administrative structure by preserving information on the previous structure.	A
K7.5	When searching for administrative unit(s), the system should also be able to find the same unit under any previous names, cfr. *Alias for administrative unit*.	A

The administrative structure is associated with the tables *Case* and *Sender/Addressee* (and thus with registry entries) in the records management module in a 1:M relationship. The association with the access-control module is a 1:M relationship with the table *Person/Role*.

7.2.2 Record structure

The record structure includes the following elements, which also make up separate tables in the data model:

- *Registry management unit:* A registry management unit (registering unit) is an organizational unit responsible for registration (entry into records) and other activities associated with the recordkeeping function and registry of the organization. A registry management unit is often associated with a particular records entity (cfr. the definition of records below), but this is not necessarily the case. In Noark-4, the relationship between registry management unit and records (records section) should be M:M. In the data model, the relationship is maintained by the table *Relationship registry management unit/records section*.

K7.6	The record-organizational structure may be different from the administrative structure, and may be described through one or more registry management units.	O
K7.7	The relationship between registry management unit and records/records section should be M:M.	O

The registry management unit is a record-organizational quantity and not part of the record structure which comprises the documents themselves.

- *Records:* This concept replaces the *partial records* of Noark-3 and Koark. It includes those documents which are produced or received by a single records creator and collected as part of his/her/its activities - also known as *records entity.* A public agency may be one records creator and thus have one records entity (centralized registry), or it may have several records creators (departments, services, etc.) which create their own records entities (partial records). If a records entity is paper-based, it comprises a physical unit. If it is electronic, it must be considered a logical unit, and the physical structure may vary considerably without affecting the logical consistency of the records.

K7.8	A records database according to the Noark standard may consist of one or more physical/logical records entities (centralized or decentralized registry).	O

- *Records section:* A records section is an arbitrarily defined section of a records entity, but it is assumed that the material in a records section is divided and sorted using a common sorting principle as primary key. The relationship between *Records* (entity) and *Records section* is 1:M. In some contexts, it may be appropriate to consider records section as synonymous with *record series*, but the two concepts are not necessarily congruent.

  The following might justify splitting a records entity into records sections:

  - To distinguish between a topic-sorted records entity and those records sections which are object-sorted (secondary systems in state filing plans, object series in the municipal K-code system). Examples of object-based records sections are personnel files ordered by name, property files sorted according to farm- and farm part-number, etc. See also *Sorting principle* below.
  - To distinguish between records sections which need different principles of periodization, cfr. chapter 12. Such division will presumably give the same result as the previous indent in most cases.
  - To distinguish between periods in the records - active records, remote records, cfr. chapter 12.
  - To distinguish between registered case documents and board documents which have not been registered (entered into records), cfr. chapter 9.

  If there is no need for such subdivision, then the entire records entity is defined as one records section.

  An important attribute in the table *Records section* is *Records status*. Among other things, *Records status* indicates if a records entity is active (status A), if it is in a transitional phase (status O) or if it is remotely stored (status B). Another attribute works as a flag which decides if it is permissible to register more cases under a records section. More detailed information is given in the technical specifications (paragraph 14.4.7).

K7.9	It should be possible to subdivide a physical/logical records entity into one or more records sections. Organizations are free to define records	O

	sections according to need.	

- *Sorting principle:* Describes the principle behind the sorting of the cases in one or more records sections. There is a 1:M relationship between sorting principle and records section. A sorting principle will normally be a filing plan code or part of a filing plan code. It may be topic-based (primary system in state keys, etc., subject codes in the K-code system) or object-based (secondary systems in state keys, etc., object types in the K-code system). If the sorting principle is also used for the division of cases (see below), this should be indicated by a separate attribute in the table.

K7.10	It should be possible to associate a primary sorting principle with each records section.	O

- *Order value:* This indicates which values are permissible within a sorting principle. There is a 1:M relationship between the two tables. It should be possible to use the order value for any type of sorting principle, be it topic-based or object-based. The concept of order value corresponds to file code or secondary code according to state filing plans, and to subject code or object code according to the K codes. To the user, i.e., in screen panels and printouts, the order values should be presented together with the prompt which the user organization has included for the sorting principle in question, for instance "file code" and "secondary code" for state filing plans, "subject code" (or possibly "department class", "common class", etc.) and "object code" for the K codes.

  It should also be easy to distinguish between primary and secondary order value. If the sorting principle is hierarchically structured (as for the standard key of the state administration), there should be a reference to the higher-level value (in the same table). For values which permit further secondary subdivision (e.g., file code 221 - Personnel files in the standard key of the state administration), there should be a reference to the secondary sorting principle.

  It should be possible to register customized values, i.e., values which have not been predefined but added by the user. Such continuous updating is mainly relevant for object-based codes.

K7.11	Order values may be object-based or topic-based.	O
K7.12	It should be possible to have hierarchically structured order values, for instance using a decimal system.	O
K7.13	A single order value should permit further subdivision according to a secondary sorting principle.	O
K7.14	It should be possible to create a separate records section for a single order value which is further subdivided according to a secondary sorting principle (e.g.,»221 Personnel files» in the standard key of the state administration, which is subdivided by name as secondary sorting principle).	O
K7.15	During coding according to filing plan, it should be permissible to use customized order values if the sorting principle so permits.	O

The order values usually have a pre-defined structure, for instance in the form of a complete filing plan. In some cases, the text relating to some order values may not

provide an adequate description of the contents of a case, and this may cause problems later on when searches are performed in the case. For this reason, it should be permissible to associate a topic word/ key word of free choice with an order value. These topic words/key words are included in a table, *Key word/topic word order value*. The topic words may be associated with the same list of topic words which is used for the document description (see chapter 5).

K7.16	It should be possible to associate one or more topic words/key words with an individual order value; searching for key words should result in the corresponding order value being retrieved and linked to the hit list.	A

- *Division of cases:* Order values should normally be applied to the case record; i.e., all registry entries and documents in the case should have the same order value. However, Noark-4 also provides for the grouping of documents within the same case by assigning different order values to the registry entries. This is called *division of cases*. The order values assigned to a registry entry must belong to a sorting principle permitted used for the division of cases, cfr. the table *Sorting principle* (paragraph 14.4.8). In screen panels and printouts, the term *case section* is used for a group of registry entries which have been assigned the same order value.

  Dividing cases is normally only a logical grouping of registry entries within a case, but it may also in some situations be necessary to divide a case physically, i.e., file individual case sections separately. Noark-4 provides for this through the registration of *records sections* for individual registry entries.

  Physically dividing a case in the records usually runs contrary to good and justified recordkeeping principles. This opportunity should not be resorted to unless there are very good reasons for it, and a physical division of cases should always be well documented. One possible usage is where cases comprise several objects, and where there is a need, *after the case has been finalized*, to file documents associated with the individual objects (e.g., person, family, property, etc.).

  If recordkeeping is electronic, the division of cases will generally be logical and thus unproblematic as far as filing is concerned. However, at the time of periodization and reorganization of the database, any case sections associated with different records sections from that of the rest of the case must be taken into account, cfr. K12.22 and K12.23.

K7.17	It should be possible to divide a case into case sections by assigning order values to the registry entries of the case.	A
K7.18	It should also be possible to associate registry entries which have been assigned a separate order value, directly with a records section which may be different from the records section with which the case is associated. This should indicate that the documents associated with the concerned registry entry have been removed from the case (for paper documents: physically) and filed in the records section and according to the order value which is registered in the registry entry.	A

7.2.3 Reference from the record structure to the records management module

Order values (file codes) are assigned to individual cases according to filing plans. Identical order values link together cases which belong together on the grounds of their subject matter. For paper-based recordkeeping, the order value is the address of the folder where the documents reside. An order value must be registered when a case is created.

In the basic version of Noark-4, there should be room for at least two order values for a case: a primary code and a secondary code. It should be possible to use both subject (topic) codes and object codes, and the user should be able to choose which code is primary and secondary. This is in line with the solution in Koark, but slightly different from Noark-3, which presupposes that object codes are always secondary. In this context, a subject code, according to the municipal K-code system, is regarded as one code with up to three components, cfr. the solution in Koark.

In an enhanced version of Noark-4, it should be possible to assign filing plan codes to a case using an arbitrary number of order values. The order values may be part of a hierarchy (primary, secondary, tertiary), or they may be independent of each other. In the data model (chapter 14), it is assumed that subject codes according to the three classes in the K-code system are treated as three separate order values, but there is nothing to stop the system from treating them as one three-component order value. See also paragraph 4.2.3, where the formal system requirements for assigning filing plan codes are included.

In order to make it possible to divide cases, the table *Registry entry* includes attributes for *Case section* (where it is possible to specify order value) and *Records section*, cfr. paragraph 14.2.8.

7.2.4 Examples of physical/logical sorting of case documents

In order to make the above principles clearer to the reader, a few examples illustrating how the record structure may work in practice follow.

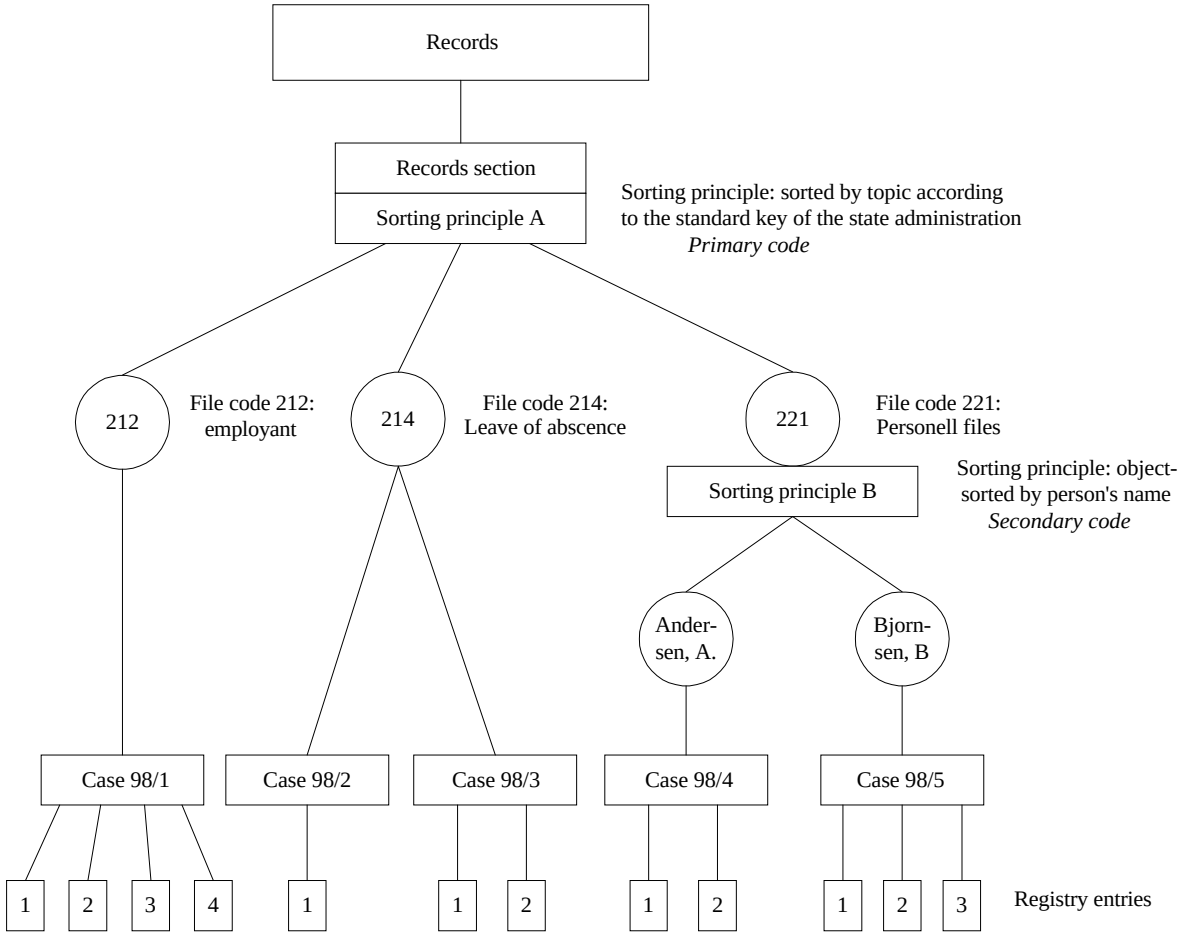


Figure 7-3: One records section, no division of cases

This records entity consists of only one records section sorted according to the standard key of the state administration, which is a topic-based filing plan based on the decimal system. Each case is assigned a file code (212, 214, etc). If the recordkeeping is paper-based, all documents which belong to a case, are stored in a folder onto which the case number has been written. The documents in the folder are sorted by document number. Each file code has its own file in the records, and in these files are put the folders in ascending order of case number. The files themselves are sorted by file code.

For file code *221 - Personnel files*, there is a break in the topic-based sorting order. The files are here sorted by "object", in this case alphabetically by the persons' family names. In the standard key of the state administration, the object codes are always secondary to the primary subject (topic) code. Cases 98/4 and 98/5 thus both have a primary and a secondary code associated with them. Still, it has been decided to let the entire records entity belong to the same records section.

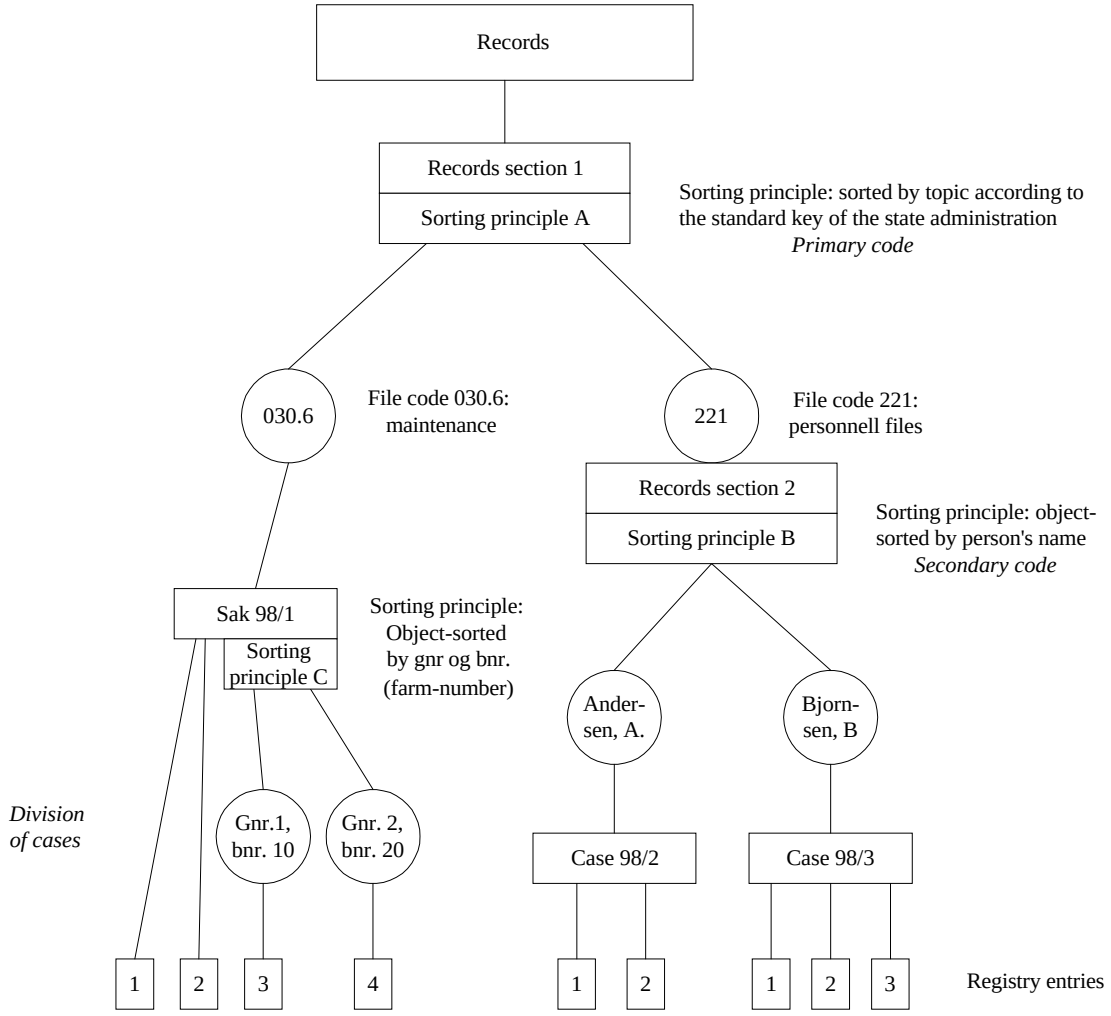


Figure 7-4: Two records sections and division of cases

The above example also uses the standard key of the state administration, but here the personnel files (file code 221) are defined as belonging to a separate records section. This is permissible because these files are sorted by another principle. One reason to have these in a separate records section may be that their periodization follows different principles from that of the topic-based records entity.

Case number 98/1 is divided by assigning separate order values to two of its registry entries; these follow a different sorting principle from that of the case itself. Registry entries 1 and 2 are only associated with the case, whereas numbers 3 and 4 have in addition been assigned an object code each - in this case the compound farm numbers used in Norway ("gårdsnummer" and "bruksnummer"). These two registry entries are thus associated with separate case sections.

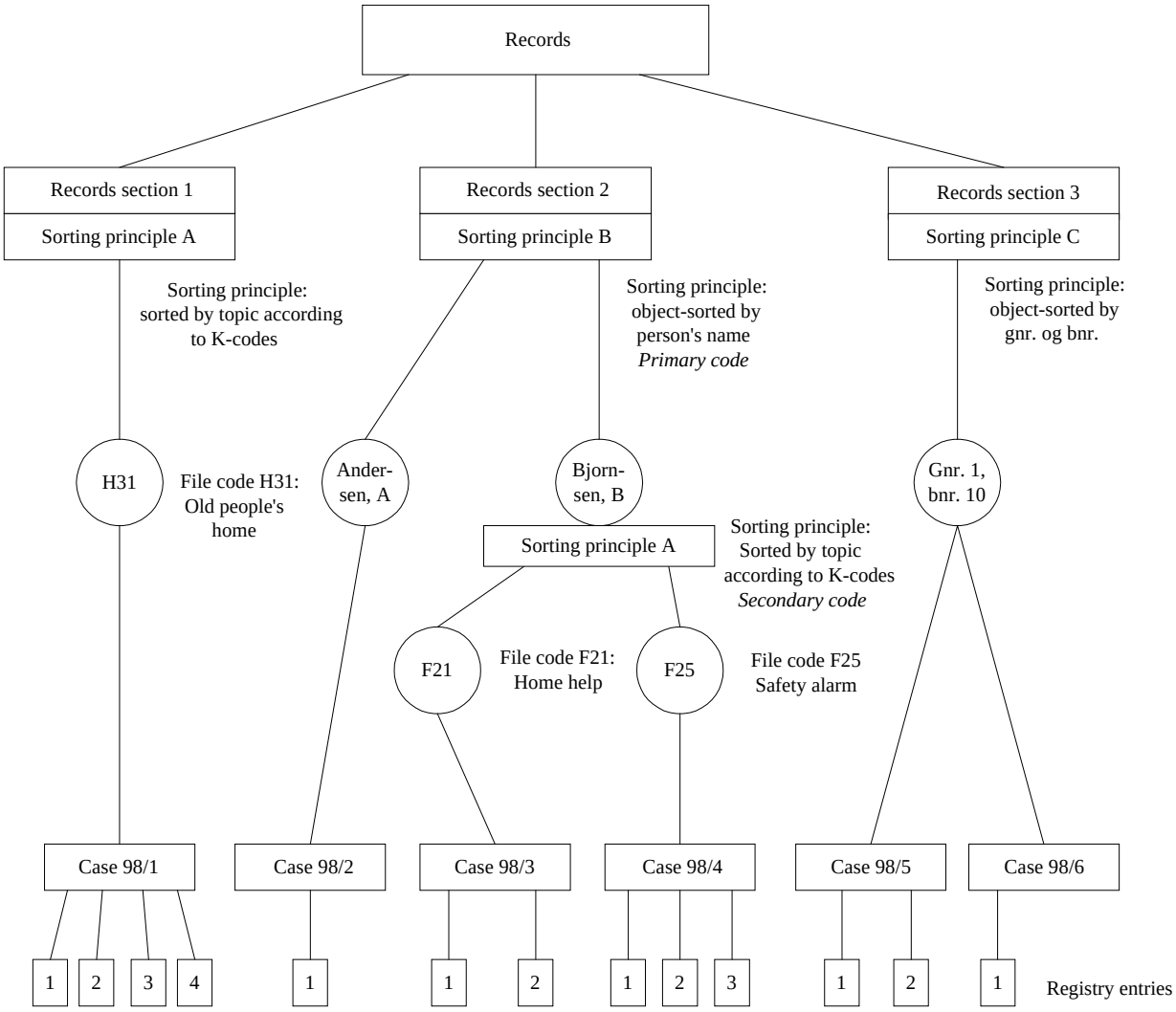


Figure 7-5: Three records sections

This records entity is sorted according to the municipal K codes. A K code is a three-component code consisting of common classes, department classes and additional classes. For filing plan codes for certain types of cases, it is permissible to combine two or three classes.

The K codes allow object codes to be primary, and in this case the records entity may be divided into three equivalent records sections sorted by different principles (one topic-based and two object-based).

It is also permissible to have secondary subject (topic) codes under the primary object code. Cases 98/3 and 98/4 are coded in this way.

7.3 Procedure requirements

The tables in the record structure module are typical auxiliary tables which must be filled with data before the system is implemented. Except for *Filing plan code*, none of the other tables are updated continuously. However, at times of reorganization, *Administrative structure*, and possibly *Registry management unit*, should be updated. Information on shut-down units should be preserved, but it should no longer be possible to use them for registration purposes. When a new filing plan is implemented, the tables *Sorting principle* and *Order value* should be updated, and the system must associate the values of the new plan with the pertinent principle. The old values should be preserved, but it should no longer be possible to use them.

7.3.1 Centralized - decentralized registry

Even if the organization has a decentralized registry with several registry management units and physical records entities, all registry data may be registered in the same database. Even for organizations with "surrounding services", a shared database may be an option. All registrars, executive officers and managers will be linked to a specific registry management unit, and it should be possible to configure the system so that they only "see" the cases which belong to these. They may, of course, be given access to search the entire database, if desirable.

The simplest way to organize the registry is by having a centralized registry where both registration and physical storage is carried out in one place. For small organizations, this is the natural thing to do. However, many large organizations have traditionally had a decentralized registry, where each department keep their own records entities ("partial records"). When a new registry system is introduced, one ought to consider whether it is still necessary to keep several records entities.

If the departments are geographically far apart, the most practical thing will still be to have one records entity (and one registry management unit) in each place - at least as long as recordkeeping is paper-based. Paper documents should always be filed close to the workplace of the executive officers.

However, as electronic recordkeeping is implemented, centralization seems natural. It is still possible to have several records entities, but each entity is then a logical unit rather than a physical one. Very large organizations - e.g., district councils with their services with separate tasks - probably ought to keep several registry management units and records entities.

Dividing a records entity into records sections should be based on functional and practical considerations. It is primarily in order to simplify procedures relating to remote storage and periodization that such division is introduced. It has previously proved difficult to remotely store a whole records entity in one operation following the same principle (i.e., the cases should be finalized). Typically, another kind of accessibility is needed for cases which are sorted by object (e.g., personnel files) than for cases sorted by topic.

7.3.2 Handling internal documents

7.3.2.1 The concept of internal documents

The concept of *internal documents* has been used in the Noark standard since it was established in 1984. Its use of the concept is based on § 5 of the Freedom of Information Act, under the heading »Unntak for interne dokumenter» [»Exemptions for internal documents»]. The first subparagraph of § 5 deals with documents »et forvaltningsorgan har utarbeidet for sin interne saksforberedelse» [»drawn up for internal preparatory purposes by an administrative body»], i.e., documents which the body prepares for its own use, and this forms the basis of the use of concepts in Noark.

However, the use of concepts in this area is not very precise. In Noark, it has been considered natural and practical to consider internal documents as documents which are communicated within an administrative unit (department, section, office, etc.) or between units which register in the same Noark base, i.e., both the sender and the addressee register their documents in the same database. In cases where the limits of a Noark base is not identical to the limits of an administrative body, the use of concepts in Noark may differ from that which is used in the Freedom of Information Act referred to above.

A further complication is the ambiguous use of this concept in the Freedom of Information Act. The second subparagraph of § 5 thus deals with documents drawn up »for et organs interne saksforberedelse» [»for internal preparatory purposes of a body»] which are prepared by a lower-level unit, by special advisers or experts or by a ministry for use by another ministry. The concept is used in a much wider sense here than in the first subparagraph. For this reason, both the Report to the Storting regarding freedom of information within public administration[6] (page 55) as well as the Archives Regulation use the concept of *"organinterne dokumenter"* (documents which are internal to the organization) about documents as referred to in the first subparagraph of § 5 of the Freedom of Information Act. However, the concept of organization is not always defined in a clear and unambiguous way, cfr. the Report to the Storting, pages 65 – 66.

With this in mind, it is necessary to emphasize how the concept of *internal document* is meant to be read in *Noark-4*. It is meant as *base-internal* documents, i.e., documents which are internal to a Noark database, or, more precisely, *documents whose sender and addressee register in the same Noark database*.

In most cases, a Noark base will cover an entire or parts of a public body. (Technically, several bodies may use the same base, but this is likely to happen only in exceptional circumstances.) Normally, internal documents in Noark-4 will be either the same as documents internal to the organization according to the Freedom of Information Act or a sub-category of such documents. In the following discussion of procedures for internal documents, internal documents in Noark-4 means internal to the organization according to the Freedom of Information Act.

Based on the above, there may be cases where external documents in Noark-4 (document types I and U) are internal to the organization according to the Freedom of Information Act. There may also be special circumstances where internal documents in Noark-4

[6] Stortingsmelding [Report to the Storting] no. 32, 1997-98.

(document types N and X, but not S) are external according to the Freedom of Information Act. These circumstances must be taken into account during the production of public register, cfr. chapter 8.

7.3.2.2 Procedures for handling internal documents

Public administration procedures for handling internal documents (i.e., internal to the organization) have been less stringent than those concerning external documents. This is partly because registering and filing internal documents has traditionally not been practised to a wide degree. When it has been done, especially in large organizations with a decentralized structure and registry, the internal documents have been treated as external. Part of the reason may be that internal documents should be available to both the sender and the addressee, who are both internal. In decentralized organizations, it has often been necessary for both the sender and the addressee to file such documents, although this is contrary to the principle of avoiding duplicate registration and filing.

The following procedures are recommended in connection with Noark-4:

- Communication between units which do not use the same Noark base, are registered as external documents of type I for incoming and U for outgoing documents, irrespective of whether the recordkeeping is paper-based or electronic, and irrespective of whether the two units are parts of the same organization or parts of different organizations.
- Communication between units which use the same Noark base, are internal according to the definition of Noark-4. These are normally registered as being of document type N, X or S, depending on what function they have. The following procedures should be followed:
- The sender should always be responsible for the registration. The document is, in other words, registered by the registry management unit to which the sender belongs. If the document has one or more addressees specified (obligatory for document type N), the registry management unit of the addressee must always be registered, so that the document is entered into the records of the addressee. If the recordkeeping is electronic, the sender should be responsible for the filing.
- If the registry management unit of the addressee is different from that of the sender, the sender should normally not register anything for the case handling attributes of the addressee. These attributes will be filled in by the registry management unit of the addressee, partly as a receipt for the received document, partly as part of the internal distribution. There may, however, be exceptions from this rule of thumb. If both dispatch and recordkeeping is electronic, and the sender knows who is going to process the document, the most appropriate thing will usually be to have the sender register everything and have the document sent straight to the executive officer for processing (after it has been filed electronically by the sender). The set of procedures to be employed should be documents in the archival plan of the organization.
- A case should always be filed together (with any exceptions which may apply for separate filing of case sections - see above). Responsibility for filing always rests with the registry management unit that created the case.
- Document type S must always be treated in accordance with the applicable procedures for documents for board handling (see chapter 9).

- If the Noark base includes several records entities and the recordkeeping is paper-based (fully or partially), it may be inconvenient to have internal documents filed in only one location. A case may be handled by two or more administrative units attached to separate records entities, only one of which contains the filed case. For those attached to the other records entities, it may be cumbersome to get hold of the relevant documents, especially if considerable geographical distances are involved. Furthermore, control is lost over the filing of documents which the unit itself has processed or produced. This problem only applies to paper-based records – electronic documents will be available to all users with the necessary access rights. The following alternative solutions may be envisaged:
- The records entity or entities which do not have archival responsibility for the case, may temporarily file documents which have been processed (received or produced) by units served by this records entity – in separate files, »memo-copybook», etc. Such temporary records material should normally be disposed of in connection with periodization and remote storage.
- One may choose to use an external document type (I or U) when registering (paper) documents which are sent between units attached to different records sections. The sender thus registers an outgoing document in one case, while the addressee registers the same document as incoming in another. Both of them file a copy of the same document in the same way as if they were communicating externally. This solution thus involves duplicate registration and filing, and it may appear untidy to have the same document registered twice in the same base. On the other hand, this solution is identical to what would have happened if the two units had used separate Noark bases, and there may be situations where two cases which partly involve the same documents, develop in different directions in the two units, especially if the two units are relatively independent of each other. It must be up to the management of the organization to decide whether to employ such solutions. If it is done, stringent procedures must be drawn up which are well documented in the archival plan.

7.3.3 Development of and changes to topic-based filing plans

When a topic-based filing plan is implemented for one or more records sections, this involves assigning to all cases in the concerned records section(s) a file code according to this plan. The file code that is assigned to a case, locates the case within a topic-based structure. For paper-based records, it also specifies physical location.

It is assumed that this structure is common to the entire records section, and that it remains unchanged as long as the records section exists – i.e., both while it is active and new cases are added to it, and after its active use ceases and it is stored remotely or transferred to archival repository. If the structure is changed, the same file code may mean different things in different cases, and the result is more or less chaos instead of structure. It is generally not acceptable to assign new filing plan codes when changes are made to the filing plan. Apart from this being a very laborious task where mistakes are easily made, a basic recordkeeping requirement stipulates that the records entity should reflect the reality that existed when the entity was created.

This involves the following requirements for procedures relating to Noark-4:

- As a rule of thumb, no changes should be made to a topic-based filing plan which has been implemented. The following exceptions apply:

  - extending the plan by introducing new file codes in a way that does not affect the codes already assigned
  - changes to the text description which complements without changing the contents.
- When it is necessary to make changes which affect file codes in use, a new (revised) filing plan is implemented, and new records sections are created where this is used. Old records sections are preserved unchanged, and the associated filing plan is preserved together with the records material.

7.4 Essential tables in the module

Only essential tables have been included here. For a full summary of the tables in this module and their attributes, see part II, Technical specifications, paragraph 14.4.

Table name	**Text**
Administrative organization	Contains a summary of administrative units, their relative hierarchy and, if appropriate, the date when they were shut down.
Records	Records entity. Describes the physical/logical records of the organization (previously called partial records).
Records section	Contains information on a part of a records entity where the material is sorted according to a common sorting principle. Records sections may have the status of active records, records in a transitional phase or remotely stored records. The table contains information on sorting principles, whether the documents are filed electronically or on paper and information concerning periodization and remote storage.
Registry management unit	Describes the organizational units responsible for registering in the records system.
Sorting principle	Contains the sorting principles (topic- or object-based) which are used or have been used as filing plans by the organization.
Order value	Contains the values which are part of a sorting principle. The order values may be hierarchically structured. Disposal rules may be associated with the individual values.

7.5 Changes from Noark-3 and Koark

Noark-4 defines an administrative structure and record structure which is much more flexible than that of Noark-3 and Koark. The major changes are presented here, and there is a complete technical description in chapter 16.

Basic version (requirement type O):

- The concept of *records* (meaning records entity) replaces the *partial records* of Noark-3 and Koark.
- The concept of *records section* is new to Noark-4, i.e., it is not used in Noark-3 or Koark. A records section is an arbitrarily defined part of a *records entity*, cfr. paragraph 7.2.2. Subdividing a records entity into records sections makes it possible, for instance, to use differentiated principles for remote storage (see chapter 12).
- In Noark-4, the relationship between *registry management unit* and *records entity* is M:M. In Noark-3 and Koark, the relationship between *registry management unit* and *partial records* is M:1.
- In Noark-4, both subject (topic) codes and object codes may be primary file codes. This also applies to Koark, but not to Noark-3.
- Noark-4 permits an unlimited number of levels in its administrative structure. In Noark-3 and Koark, this was limited to 2 - 3.

Enhanced version (requirement type O1):

- A case in Noark-4 may be assigned a filing plan code with an arbitrary number of *order values* (file codes). These may be organized hierarchically (primary, secondary, tertiary), but it is also possible to register additional codes outside the hierarchy. In Noark-3 and Koark, the number of file codes is limited.

Recommended functionality (requirement type A):

- The option of *dividing cases* (into *case sections*) is new to Noark-4.

8. MODULE FOR ACCESS CONTROL AND USER MANAGEMENT

8.1 Purpose of module

This module is used to control access to reading, registering and updating various kinds of information which is stored in the database.

The system is to provide for the management of users and their association with administrative units. It should differentiate the individual users' read and right access- both with regard to their administrative ties and their roles and responsibilities as managers and executive officers.

The system should have functions for screening information which is to be subject to provisions concerning exemption from public access and the protection of personal integrity, etc. This should make it possible to regulate public access to records information and case documents, in accordance with the provisions of the Freedom of Information Act.

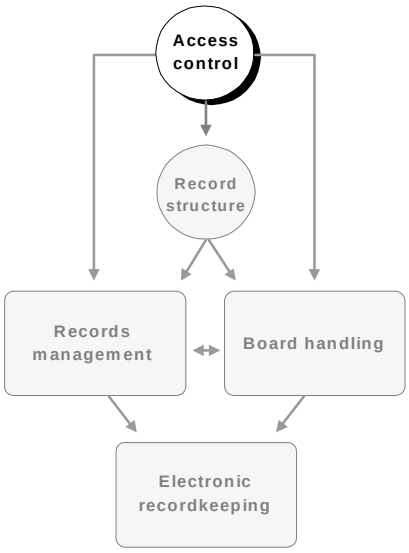


Figure 8-1: Position of access-control module in Noark

The main purpose of the module may be summarized as follows:

- To ensure that the right person in the right position is given the access necessary to perform tasks
- To prevent intruders from gaining access to screened-off information
- To guarantee the public's statutory right to access to information

Electronic case handling and recordkeeping provides for changes in the division of labour between executive officers and the centralized recordkeeping services. New functions for registration and storage - of drafts, notes, remarks, logging of document flow and finalized case documents - are intimately connected with the production process itself, and presuppose that executive officers contribute in a more direct way than before. Such contribution is in many areas necessary in order to implement the new functions. Increased opportunities for the executive officers to carry out the registration and updating themselves may, however, increase the risk of having incorrect or incomplete information registered in the system, and possibly of reducing data integrity. In order to prevent such consequences from the increased delegation of responsibility and authority, the system has been enhanced with several new *quality-control functions*:

- more detailed access control
- stricter process-management procedures which regulate when and in what order the individual users perform their registration tasks

- identification of the persons responsible for performing specific tasks
- logging of completed changes in well-defined function areas
- centralized verification of performed tasks and registered information

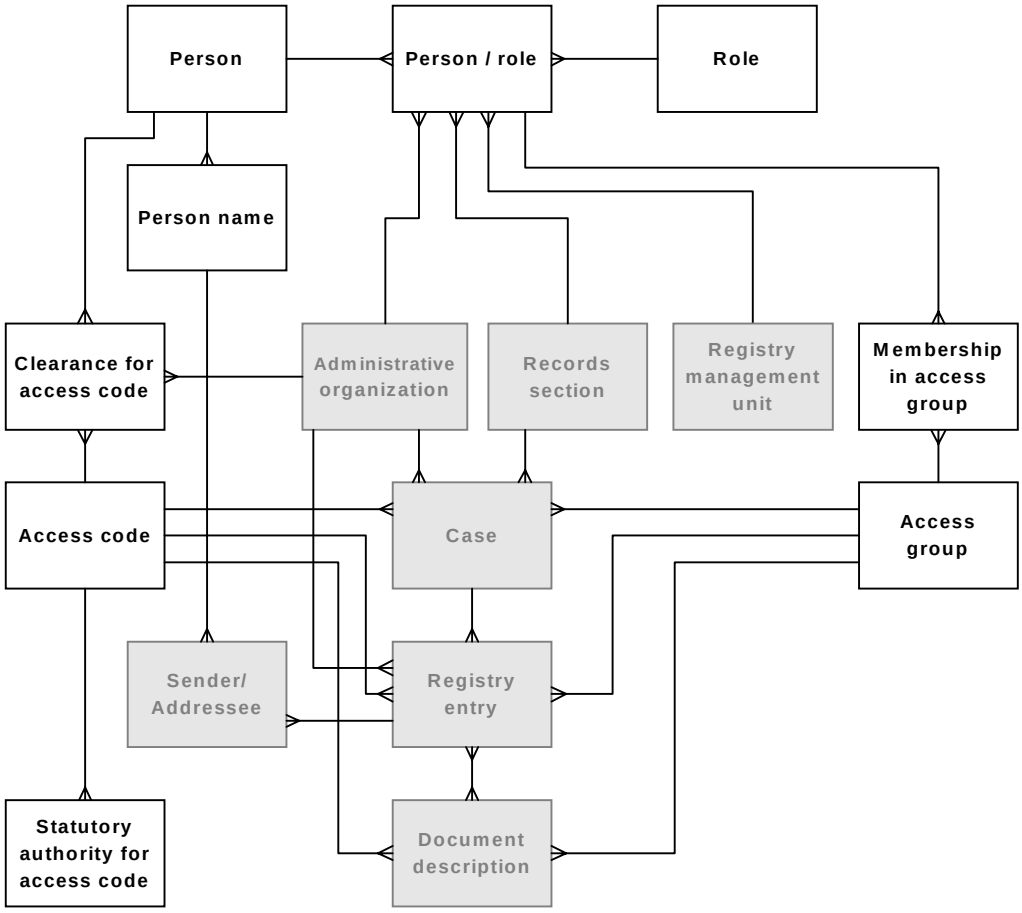
8.2 Module design

The essential tables in this module are *Person, Person-Role* and *Role*. *Person* describes all the persons within the organization who have rights within the system, persons who have had rights within the system and persons to whom references are made from one or more records within the system (as executive officer, board member, etc.). The table *Person* also handles history with regard to name changes, etc., by linking up to *Person name*. *Person-Role* associates a person with a role, and *Role* contains information on the rights associated with the individual roles.

Other important tables are *Clearance for access code*, which authorizes users for access to screened information, and *Membership in access group*, which makes it possible to screen the information access to specified groups of users according to need.

The following figure shows important tables included in the module as white boxes. The gray boxes are tables from other modules which are necessary for demonstrating the logic of the system.

Figure 8-2: Module for access control and user management



8.2.1 User management

The user management is a basic security function in the Noark system. It determines what functions may be performed by whom, which is essential to the data quality of the base. It also determines who gets access to what information. This must function adequately for it to be advisable to register and store sensitive information in the base. The following general requirements apply to the user administration in Noark-4:

K8.1	The module for access control and user management should control and survey all use of the system. The users should only be able to use functions and information for which they are authorized. Authorization and verification is controlled by the information content in the tables of the module.	O
K8.2	At logon, all users should identify themselves by a user identification controlled by the system. The user identification should give the system the necessary access to information concerning the user's rights and restrictions.	O
K8.3	The functions to which the user has access should, as far as possible and appropriate, appear from the individual panels (e.g., through the use of different colours, shades of grey, etc., on icons).	A
K8.4	The same person (user) should be able to use different names and initials, e.g., after changing his/her name. It should be possible to preserve all names and initials in the system as well as information on periods of use. The system should keep track of names and initials which belong to the same person (see the tables *Person* and *Person name*).	O
K8.5	It should be possible to decide that a person (secretary) may register on behalf of somebody else, and with the same rights as that person.	A
K8.6	The system should always provide for "alias" searches for all names and initials associated with a person. Searches for names should, in such cases, include all names associated with the person concerned. It should also be possible to disable the "alias" function.	A

The rights and restrictions of the users are associated with their roles:

K8.7	A user of the system should be associated with one or more roles, each giving specific rights. The user's association with a role should be limited to a specific period of time (from date to date).	O
K8.8	The user's right in connection with a role should be defined globally, i.e., for the entire database, or within a registry management unit.	O1
K8.9	One of the roles with which the user is associated, should be defined as his/her normal role, i.e., the role which the user will play unless otherwise specified.	O
K8.10	It should be possible to associate a person in a specific role with an administrative unit, a registry management unit and a records section (table: *Person-Role*). It should be possible to use these units as default values when the user performs registrations which involve these attributes.	O

8.2.2 Managing write access

Write access in the Noark base includes the right to:
- register and modify information
- perform specific functions, such as create a new case or registry entry, etc.

Write access is managed through:
- general rights and restrictions associated with individual roles
- rights and restrictions for the individual roles at the various process stages of the document handling (see chapter 6).

8.2.2.1 Roles and associated rights

Noark-4 defines a set of default roles with specific rights and restrictions. It should, however, be possible to introduce further differentiation according to the needs of the organization.

K8.11	As a default, the following roles should be defined in the system (the corresponding user types in Noark-3 and Koark are indicated in brackets): *Role 0 - SY:* System administrator (Koark: 0) *Role 1 - AR1:* Registry administrator (Koark: 1, Noark-3: 1) *Role 2 - AR2:* Registry personnel (Koark: 2) *Role 3 - LD:* Manager/case distributor (Koark: 3, Noark-3: 2) *Role 4 - SB:* Executive officer (Koark: 4, Noark-3: 3) *Role 5 - US:* Board secretary (Koark: 5) *Role 6 - AN:* Other (Koark: 6, Noark-3: 4). *Role 7 - EKS:* External (Koark: included in 6, Noark-3: included in 4). *Role 5* only applies to the board-handling module (*requirement type U*). *Role 7* only applies when the recommended functions for giving external users access to the base, have been included, cfr. K8.89 - K8.90 (*requirement type A*).	O
K8.12	It should be possible to define other roles in addition to these. When this is done, it should be possible to use a default role as starting point and then edit it.	O1
K8.13	It should be possible to register the individual rights which may be associated with a role, in separate attributes, in accordance with the specifications in the table *Role*, or by other means which provide similar flexibility.	O1
K8.14	It should not be possible to create roles which unblock the general restrictions of the system.	O

The following general rights and restrictions should be associated with the individual default roles (note that all rights are limited by the restrictions associated with the individual attributes in chapter 14):

K8.15	*Role 0 - SY (System administrator):* • Rights: - access to all system and operating functions - the right to authorize himself/herself and other users for all types of rights • Restrictions: - no access to registration and correction functions in the records management module, electronic recordkeeping, record structure module and board-handling module	O
K8.16	*Role 1 - AR1(Registry administrator):* • Rights: - permission to create cases, registry entries and electronic documents - permission to file and dispatch electronic documents - access to all registration and correction functions (including moving registry entries) in the records management module, electronic records and record structure module - the right to authorize himself/herself and other users for registering in the same three modules, as well as access codes and association with access groups - the rights apply to the entire Noark base • Restrictions: - the authorization right for access codes only applies to the codes for which the person himself/herself is authorized - the right to register and make corrections is restricted by the process-management rules (see below) - the right to register and make corrections in the electronic records does not include the right to modify filed documents	O
K8.17	*Role 2 - AR2 (Registry personnel):* • Rights: - permission to create cases, registry entries and electronic documents - permission to file and dispatch electronic documents - access to all registration and correction functions (including moving registry entries) in the records management module and electronic records - permission to associate users with access groups • Restrictions: - the right to register and make corrections is restricted by the process-management rules (see below) - the right to register and make corrections in the electronic records does not include the right to modify filed documents - all registration functions and write access are limited to the person's own registry management unit	O

K8.18	*Role 3 - LD (Manager/case distributor):* • Rights: - permission to create cases, registry entries and documents - access to registration and correction functions in the records management module and electronic records according to the process-management rules (see 8.2.2.2 and chapter 6) - permission to register notes - permission to register handling plan for board handling in a case - the right to authorize executive officers for registration in accordance with the rights and restrictions of role 4 - SB (cfr. K8.19), as well as for access codes and membership in access groups • Restrictions: - the authorization right for access codes only applies to the codes for which the person himself/herself is authorized - the right to create registry entries is limited to cases associated with the person's administrative unit or units subordinate to it, or to cases where there already exist registry entries associated with this/these unit(s) - all other registration functions and write access are limited to the person's own registry management unit or units which are subordinate to it.	O
K8.19	*Role 4 - SB (Executive officer):* • Rights: - permission to create cases, registry entries and documents - access to registration and correction functions in the records management module and electronic records according to the process-management rules (see 8.2.2.2 and chapter 6) - permission to register notes - permission to register handling plan for board handling in a case (for which the person is case-responsible) - the right to create ad-hoc access groups associated with cases for which the person is case-responsible, or with registry entries for which the person is executive officer • Restrictions: - the right to create registry entries is limited to cases for which the person is case-responsible, or to cases where there are already registry entries for which the person is executive officer - all other registration functions and write access are limited to cases for which the person is case-responsible, or to registry entries and their associated documents for which the person is executive officer	O

K8.20	*Role 5 - US (Board secretary):* • Rights: - access to all functions for registering, correcting, filing, etc., in the board-handling module - the same rights as SB for document type S in the records management module and electronic records (see below concerning process management) - permission to register notes • Restrictions: - the registration functions and write access in the board-handling module are limited to the board(s) for which the person is registered as secretary - the write access in the board-handling module is limited to the documents for which the person is registered as executive officer	U
K8.21	*Role 6 - AN (Other),* *Role 7 – EKS (External):* No write access	O

Note: *K8.15 – K8.19 as well as K8.21 are designated type O, even if they also refer to some modules and functions which are not included in the basic version of Noark-4. This means that the rights in question must be considered obligatory where relevant. For instance, requirements concerning notes and electronic records are to be considered as O2 requirements.*

8.2.2.2 Rights at various process stages in document processing

Chapter 6 describes various process courses in connection with document handling, what parties are involved and what rights and responsibilities they have at various stages of the handling process. The description uses the process itself as its starting point and place the various parties with their rights and responsibilities in relation to this. This chapter starts off from the individual persons involved and summarizes their rights and restrictions at various stages of the process.

Chapter 6 operates with three types of parties (persons) in connection with document handling. They correspond to the above user roles as follows:

- AR (registry office) includes both AR1 and AR2 (roles 1 and 2). They have the same rights in the handling process, but the rights of AR2 are generally limited to his/her own registry management unit, while AR1 may operate in the entire Noark base.
- LD (manager) corresponds to the role of LD (role 3).
- SB (executive officer) corresponds to the role of SB (role 4). Note that US (role 5) has the same rights as SB for document type S.

The following description uses the designations AR, LD and SB. Their general rights and restrictions follow the specification of requirements in 8.2.2.1 above.

Process-related rights and restrictions for AR (roles AR1 and AR2):

K8.22	Case status = R, B, X	The general rights and restrictions for AR apply in their entirety.	O
K8.23	Case status = A	The following restrictions in the general rights apply to AR: • AR may only modify the following attributes in or associated with the table *Case:* - *Case status* - attributes for access control - attributes for precedent - attributes for disposal - attributes associated with *Cfr. case* - *(Re)activation (date)* - lending attributes - *Records section* (only as part of a move according to the specifications of K12.5 and K12.6) • AR may not create new registry entries in the case or associate new electronic documents. • AR may not dispatch or file electronic documents associated with the case.	O
K8.24	Case status = U	AR may modify the attribute *Case status*. All other registration functions are blocked.	O
K8.25	Registry status = M, S, R, F, E, J	The general rights and restrictions for AR apply in their entirety.	O1
K8.26	Registry status = A	The following restrictions in the general rights apply to AR: • AR may only modify the following attributes in or associated with the table *Registry entry:* - *Registry status* - Attributes for access control - Attributes for lending - *Records section* (only as part of a move according to the specifications of K12.5 and K12.6) • AR may not associate new electronic documents with the registry entry. • AR may not dispatch or file electronic documents associated with the case.	O1
K8.27	Registry status = U	AR may modify *Registry status*, but has no registration rights beyond this.	O1
K8.28	Document status = B (or equivalent)	AR has no registration rights in the tables *Document description* and *Version*.	O2
K8.29	Document status = F	The general rights and restrictions for AR apply in their entirety.	O2

Process-related rights and restrictions for LD and SB:

K8.30	Case status = R	Process-related rights for LD and SB: • The general rights and restrictions apply. • LD/SB may register in all attributes in the tables *Case* and *Part in case* (if implemented).	O
K8.31	Case status = B, X	Process-related rights for LD and SB: • LD/SB may modify the following attributes in or associated with the table *Case:* - attributes in *Part in case* (if implemented) - attributes associated with *Cfr. case* - attributes for access control - attributes for precedent - *(Re)activation (date)* • LD/SB may create new registry entries in the case.	O
K8.32	Case status = A	Process-related rights for LD and SB: • LD/SB may modify the following attributes in or associated with the table *Case:* - attributes for access control - attributes for precedent - *(Re)activation (date)*	O
K8.33	Case status = U	LD/SB do not have access to registration functions in the case.	O
K8.34	Registry status = M	Process-related rights for LD and SB: They may register in all attributes in the tables *Registry entry* and *Sender/Addressee*.	O1
K8.35	Registry status = S, R	Process-related rights for LD and SB: • LD/SB may register in all attributes in the tables *Registry entry* and *Sender/Addressee.* • LD/SB may associate electronic documents with the registry entry.	O1
K8.36	Registry status = F	Process-related rights for LD and SB: • LD/SB may modify the following attributes in the tables *Registry entry* and *Sender/Addressee:* - *Registry status* (to the values **R** or **E**) - attributes for access control - *Executive officer* (only LD) - *Maturity date* and *Processing deadline* (only LD) - attributes for depreciation • LD/SB may dispatch and file electronic documents associated with the registry entry.	O2
K8.37	Registry status = E	Process-related rights for LD and SB: • LD/SB may modify the following attributes in the tables *Registry entry* and *Sender/Addressee:* - *Registry status* (to the values **R** or **F**) - attributes for access control - *Executive officer* (only LD) - *Maturity date* and *Processing deadline* (only LD)	O2

		- attributes for depreciation • LD/SB may dispatch to CC addressees and file electronic documents associated with the registry entry.	
K8.38	Registry status = J	Process-related rights for LD and SB: • LD/SB may modify the following attributes in the tables *Registry entry* and *Sender/Addressee:* - attributes for access control - *Executive officer* (only LD) - *Maturity date* and *Processing deadline* (only LD) - attributes for depreciation	O1
K8.39	Registry status = A	Process-related rights for LD and SB: • LD/SB may modify the following attributes in the table *Registry entry:* - attributes for access control	O1
K8.40	Registry status = U	No registration rights for LD/SB.	O1
K8.41	Document status = B (or equivalent)	Process-related rights for LD and SB: They may register in all available attributes in the tables *Document description* and *Version* as well as file new versions of the document.	O2
K8.42	Document status = F	Process-related rights for LD and SB: • LD/SB may modify the following attributes in the table *Document description:* - *Document status* (on certain conditions - see K6.30) - attributes for access control	O2

8.2.3 Managing read access

The access control of Noark-4 regulates the read access to the information in the database. This applies to all kinds of information - records management information (including records information), documents in the electronic records and all kinds of background information concerning administrative structure, record structure, user roles, etc.

Noark-4 assumes that the information in the base is open to all users. However, it contains several functions for screening of information to which not everybody should have access. Such screening may be relevant for information which is subject to exemption from public access according to laws and regulations, and it may be resorted to for information which the organization - for other reasons - prefers not to distribute to all its users.

Screening of information is closely related to the provisions of the Freedom of Information Act and its regulations. The access control of Noark-4 is designed with an eye on these provisions, and it provides the necessary flexibility to carry out the screening according to the letter and intention of the act. The way in which the screening is carried out, however, cannot be governed by Noark. It will depend on the procedures set up by the individual user organization and the way in which the users (managers, registry personnel, etc.)

practise the established procedures. This is discussed in more detail in paragraph 8.3.3 below.

The provisions of the Freedom of Information Act regulate *public* access to records information and case documents. However, the way in which a public body regulates access to information for the *users in the Noark system* (hereafter referred to as internal users), is not covered by the Freedom of Information Act. This is up to the organization itself, as long as any provisions on confidentiality, protection of personal integrity, etc., are respected.

In the context of Noark, it seems natural to emphasize the importance of giving as many internal users as possible access to the information in the base (that which is not subject to professional secrecy). However, there may also be organizations which need to limit read access, especially for internal documents and other internal information, to those parts of the records base which are associated with the users' own administrative or record-organizational unit(s). This may for instance apply to large or complex organizations which share a Noark base, such as a state office which covers the entire country, the entire local administration of a large district council, etc. In some cases, such limitation may be necessary in order not to be subject to licensing according to the Personal Data Registers Act, cfr. the *Personal Data Registers Regulation, § 2-19 on electronic records*.

This sub-chapter deals with the management of read access in the records management module and electronic records. The read access in the board-handling module are discussed as part of a complete presentation of that module in chapter 9.

8.2.3.1 Screening functions in a Noark system

There are two principles for screening in Noark-4:

1) Screening based on access codes (corresponds to "grad-koder" (grading codes) in Noark-3 and Koark):

This is used to screen registered information or individual documents. The screening enters into force when an access code is applied to an individual case, registry entry or document. The system users must be *cleared* for specific access codes and *authorized* for a defined part of the cases and registry entries and their associated documents which are screened using individual access codes. Only users who are cleared for a specific access code and authorized for the concerned case and/or registry entry, may see the information which is screened using this code. The information to be screened in a case, registry entry or document is indicated by checking off, cfr. 8.2.3.3 below. All other information is open to everybody (within the context of access according to administrative or record-organizational criteria - see no. 2 below). The access codes to be used are described in paragraph 8.2.3.2.

Within the framework of the individual access code, the following opportunities exist for *authorizing* users (cfr. the table *Clearance for access code*):

- The default, which is implicit in the *clearance* for an access code, is that the user is authorized for information and documents within the cases for which he/she is case-responsible, as well as for information and documents in registry entries for which he/she is executive officer.

- The authorization may be extended by authorizing the user for information and documents within one or more administrative units as well as those units which are subordinate to them. The authorization may be defined in different ways for different access codes.
- The authorization may be further extended by associating the user with an *access group* and by using this access group in combination with the person's access code. Access groups are used to authorize users for access to individual cases, registry entries or documents across the administrative organization, case-responsibility, etc. Access groups may be defined on a general basis (e.g.,»security board»), and an arbitrary number of cases, registry entries or documents may be associated with them. Access groups may also be defined ad hoc and be associated with a specific case or registry entry.

2) Screening based on administrative or record-organizational criteria:

This screening function should make it possible to limit the read access of the user to specific parts of the Noark base. The rights may be limited according to record-organizational criteria, based on the *registry entry*, or according to other administrative criteria, i.e., based on the *administrative unit including subordinate units*. Within the specified units, the user is given access to all information and all documents, with the restrictions that follow from the access codes and the authorization associated with these, cfr. no. 1 above. Outside the specified units, all information is blocked for the user.

Noark-4 does not pose specific requirements with regard to the layout of such a solution, or to whether record-organizational or administrative criteria should be used. The only requirement is that there should be a solution which makes it possible to limit read access to specific parts of the base according to general record-organizational or administrative criteria, cfr. K8.53.

It is up to the organization itself to decide what screening functions should be implemented. However, it is not recommended to use more functions than necessary. In small organizations, it will usually suffice to use access codes, especially if there is not a lot of sensitive information. For large organizations which process much and varied sensitive information, on the other hand, it may be appropriate to combine several screening functions.

Note: *When an executive officer or manager is given access to specific registry entries (with their associated documents) which are associated with units outside the person's authorization, the simplest thing will often be to define the person as CC addressee, cfr. paragraph 4.2.6. This may result in the person obtaining status as executive officer for the specific registry entry and thus read access to information and documents, within the framework provided by the access code.*

The system should provide for the following general functions for managing read access:

K8.43	It should be possible to register access codes for cases, registry entries and documents. The code indicates that registered information or filed documents should be screened against unauthorized access. The information to be screened and the ways of indicating this are specified in paragraph 8.2.3.3.	O
K8.44	It should be possible to *clear* an individual user for one or more access	O

	codes, cfr. the table *Clearance for access code*. In the basic version of Noark-4, users who are cleared for an access code should automatically be *authorized* to see all information which is screened with this code, possibly limited to the record-organizational or administrative units which are specified in accordance with K8.53. Users who are not cleared for an access code, may not read information screened with this code. This also applies to previously registered information if a user's clearance is withdrawn for the access code in question.	
K8.45	In an enhanced version of Noark-4, users who are cleared for an access code, should always be *authorized* for this within parts of the Noark base, cfr. the table *Authorization within administrative unit*. The authorization should be defined according to one of the following options: • *Default authorization*, limited to cases for which the user is case-responsible or registry entries for which he/she is executive officer (both including associated information and documents). Default authorization is set automatically when the user is cleared for the access code. • *Enhanced authorization*, limited to one or more administrative units and the units subordinate to them. If the authorization is to apply to the entire organization, the organization should be defined as administrative unit.	O1
K8.46	It should be possible to register a user as member of an access group, cfr. the table *Membership in access group*, and it should be possible to associate cases, registry entries and documents with an access group, cfr. the attribute *Access group* in the respective tables. Membership in an access group should authorize a user for access to information in those cases, registry entries and documents which are associated with the group, provided that the user is cleared for the access code indicated on the case, registry entry or document.	O1
K8.47	It should be possible to carry out the registration of access groups and membership in these, i.e., adding or removing members, in a separate operation. It should also be possible to carry out such registration in connection with the registration or correction of information in a case or registry entry.	O1
K8.48	A user should not be able to enter access codes for which he or she is not cleared himself/herself. Neither should the user be able to register or correct information in cases, registry entires or document descriptions for which he/she is not authorized.	O
K8.49	The system should prevent a case from having a case-responsible assigned who is not cleared for the access codes which are used in the case (including associated registry entries and documents, etc.). Likewise, the system should prevent a registry entry from having an executive officer assigned who is not cleared for the access codes used in the registry entry (including associated documents, etc.).	O
K8.50	As long as a case is not finalized (i.e., as long as *Case status* is different from **A**), the system should prevent the case (including associated registry entries and documents, etc.) from having an access code assigned for which the case-responsible is not cleared. When *Case status* is **A**, the system should allow such registration, but only after the	O

	user has provided a confirmatory answer to a control question.	
K8.51	As long as a registry entry is not finalized (i.e., as long as *Registry status* is different from **A**), the system should prevent the registry entry (including associated documents, etc.) from having an access code assigned for which the executive officer is not cleared. When *Registry status* is **A**, the system should allow such registration, but only after the user has provided a confirmatory answer to a control question.	O
K8.52	If a user's authorization or clearance is withdrawn, the system should issue a warning if the concerned person loses his/her access to cases/registry entries for which he/she is case-responsible or executive officer. If any of the cases or registry entries are not finalized, a confirmatory answer must be given to a control question before the change can be effectuated.	O1
K8.53	It should be possible to limit a user's read access to parts of the Noark base according to record-organizational criteria (one or more registry management units) or according to administrative criteria (one or more administrative units including subordinate units). It is optional whether both types of criteria should be permitted or only one type.	O1

8.2.3.2 Access codes and their statutory authority

The use of an access code for a case, registry entry or document has the following consequences:

- certain information is unavailable to internal users who are not cleared for the code in question
- this information is not included in the public registry, cfr. 8.2.3.5 below

It follows from the last indent that any use of access codes must be warranted in the Freedom of Information Act, and that it must be possible to indicate the statutory authority at request.

Noark-4 leaves it up to the individual organization to define what access codes will be used. However, all access codes should be registered in the system (by users who are authorized for such registration) before they are used, and they should relate to a statutory authority based on §§ 4, 5, 5a, 6 or 11 of the Freedom of Information Act.

K8.54	For it to be permissible to assign an access code to a case, registry entry or document, the code must be predefined (registered) in the system, cfr. the table *Access code*.	O
K8.55	Access codes which are defined in the system, are not valid unless there is a registered statutory authority for the code, cfr. the table *Statutory authority for access code*. Exempted from this requirement is access code XX (temporarily blocked), cfr. below.	O
K8.56	When an access code is registered for a case, registry entry or document, the system should automatically retrieve the corresponding statutory authority and add it to the relevant attribute of the case, registry entry or document. In order to remind the user that the automatically retrieved authority is not always complete, the prompt should be placed after the last character in the statutory authority field on the screen.	O

In Noark-4, some access codes and statutory authorities have been predefined. These codes should always exist in a Noark system, and they should (if possible) be blocked against changes. The codes are associated with fixed systems such as the safety instruction and the security and protection instruction as well as the individual paragraphs concerning exemptions in the Freedom of Information Act. Furthermore, a code has been added for temporary blocking information pending a decision as to whether the general public should have access to the information.

K8.57	The following access codes and their statutory authorities should be predefined in a Noark system. The individual organization should be able to add or remove codes according to need.	O

Code	***Description***	***Statutory authority***
B	Restricted according to the Safety Instruction	Freedom of Information Act § 6.1, Safety Instruction
K	Confidential according to the Safety Instruction	Freedom of Information Act § 6.1, Safety Instruction
H	Secret according to the Safety Instruction	Freedom of Information Act § 6.1, Safety Instruction
F	"Fortrolig" (confidential) according to the Security and Protection Instruction	Freedom of Information Act § 5a, Security and Protection Instruction
SF	"Strengt fortrolig" (strictly confidential) according to the Security and Protection Instruction	Freedom of Information Act § 5a, Security and Protection Instruction
4	Public access delayed in accordance with the Freedom of Information Act, § 4 (to be specified)	Freedom of Information Act § 4
5	Exempt from public access in accordance with the Freedom of Information Act, § 5 (statutory authority must be further specified)	Freedom of Information Act § 5
5a	Exempt from public access in accordance with the Freedom of Information Act, § 5a (statutory authority must be further specified)	Freedom of Information Act § 5a
6	Exempt from public access in accordance with the Freedom of Information Act, § 6 (statutory authority must be further specified)	Freedom of Information Act § 6
11	Exempt from public access in accordance with the Freedom of Information Act, § 11 (statutory authority in regulation must be further specified)	Freedom of Information Act § 11
XX	Temporarily blocked	

K8.58	The codes B, K and H should be grouped together in a hierarchy with H on top and B at the bottom. This should result in all users who are authorized for H being automatically authorized for K and B, etc. A similar hierarchy should be defined for the codes F and SF, where SF is the highest.	A
K8.59	It should be possible to define similar hierarchies for other sets of access codes.	A

The codes 5, 5a and 6 are general codes for information which is exempt from public access according to the three paragraphs in the Freedom of Information Act. This may suffice for organizations which have little material for screening. However, in many cases it may be appropriate to use a higher number of more specialized codes for information to be screened, e.g., P for personnel cases, KL for client cases, etc. In this way, exemption from public access may be combined with screening from internal user groups (for instance so that only the personnel department and certain managers are authorized for code P, etc.).

When statutory authority is specified, the setup may be as follows:

Code	***Description***	***Statutory authority***
P	Personnel cases	Freedom of Information Act § 5a, Public Administration Act § 13.
KL	Client cases	Freedom of Information Act § 5a, Public Administration Act § 13.

On the other hand, it soon becomes difficult to keep track if too many different access codes are used. If there is a need for highly differentiated screening, it is recommended that differentiated authorization of users be used within the individual access codes, administratively or using access groups.

Access code XX is an exception. It is applied automatically by the system to all newly registered cases, registry entries and documents, and indicates that the information is blocked until a decision has been made with regard to public access/screening. This is described in more detail in 8.2.3.4. Code XX does not entail exemption from public access, only a temporary delay, in accordance with current good practice and without affecting the provisions of the Freedom of Information Act. No statutory authority has thus been specified for this code, cfr. K8.55 above.

8.2.3.3 Screening of individual pieces of information and documents

Screening based on *record-organizational or administrative criteria* includes all information in cases, registry entries and case documents which are not associated with the concerned units, cfr. K8.53 above. The screening enters into force the moment the administrative and/or record-organizational position of the case or registry entry is established.

Screening according to *access code* only applies to a set of information within the concerned case or registry entry, as well as any complete case documents. The access code is assigned when the case or registry entry is registered, or possibly later.

K8.60	It should be possible to screen the following case information using an access code: • Parts of the case title (*Case title* in the table *Case*): the system should either permit the screening of everything but the first part of the title (e.g., the first line) or screening of individual words which the user highlights. • File codes/filing plan codes (*Order value* in the table *Filing plan code*): This is primarily intended for the screening of object codes which are person names. • Information which identifies parts in a case (the entire table *Part in case*).	O
K8.61	It should be possible to screen the following information associated with a registry entry using an access code: • Parts of the description of contents (*Description of contents* in the table *Registry entry*): The system should either permit the screening of everything but the first part of the description of contents (e.g., the first line) or screening of individual words which the user highlights. • Case part (*Case part* in the table *Registry entry*): Used e.g. when a case part is specified using an object code which is a person name. • Information which identifies the sender and/or addressee (the attributes *Name, Short name, Address, E-mail address, Reference* in the table *Sender/Addressee*).	O
K8.62	It should be possible to screen the following information associated with electronic documents using an access code: • All information concerning a document in the tables *Document description* and *Version* as well as the document itself (the text) is screened together, i.e., it is checked off once. Excepted from screening is the public version of the document, if such a version exists (the attribute *Variant* in the table *Version* = O).	O2
K8.63	It should be possible to screen notes, cfr. the table *Note*. The screening of a note should include all its information.	O2
K8.64	It should be possible to screen additional information, cfr. the table *Additional information*. The screening should include all information.	O1
K8.65	It should be possible to screen information on precedent, cfr. the table *Precedent*. The screening should include all information.	O

When a user registers an access code, the following functionality for the screening of information should be provided:

K8.66	The user should be able to check off what information is to be screened. It should then be possible for the system to show what information is checked off, in all contexts where this is appropriate.	O
K8.67	It should be possible to check off collectively the information to be screened, for instance by using the number codes specified in Noark-3 and Koark.	A

K8.68	When an access code is registered for a case, it should be possible to check off for the screening of information related to the case, cfr. K8.60.	O
K8.69	When there are several parts in a case, it should be possible to screen them individually, but it should also be possible to check them off collectively.	O1
K8.70	When an access code is registered for a registry entry, it should be possible to check off for the screening of information related to the registry entry as well as for electronic documents associated with the registry entry, cfr. K8.61 and K8.62.	O
K8.71	When a registry entry has several senders or addressees, it should be possible to screen these individually, but it should also be possible to check them off collectively.	O1
K8.72	The screening of registered electronic documents should always be carried out from a registry entry with which they are associated. It should be possible to register an access code for the registry entry when the associated documents are to be screened, without having to check off any of the records information for screening, cfr. screening code 1 in Noark-3 and Koark.	O2
K8.73	The electronic main document of a registry entry should always have the same access code and (if applicable) the same access group as the registry entry. The values are inherited when the registry entry is registered or modified, and it should not be possible to modify them in any other way.	O2
K8.74	Electronic documents which are not main documents of a registry entry, should inherit the access code and any access group of the registry entry as default value, unless they have already been assigned an access code or access group and provided they are not already associated with another registry entry. If no access code or access group is inherited when a registry entry is registered or modified, the user should be notified. It should be possible to modify the access code and any access group for documents which are not main documents of a registry entry.	O2
K8.75	Notes (see K8.63) should inherit the access code and any access group from the case, registry entry or document with which they are associated. It should be possible to modify the values.	O2
K8.76	Additional information (see K8.64) should inherit the access code and any access group from the case, registry entry or document with which it is associated. It should be possible to modify the values.	O1
K8.77	Precedents (see K8.65) should inherit the access code and any access group from the case with which they are associated. It should be possible to modify the values.	O
K8.78	Except as specified in K8.73 – K8.77, access codes and access groups should not be inherited from one level to the next (e.g., from case to registry entry).	O
K8.79	Only information which is checked off for screening, should be screened against access by unauthorized users.	O
K8.80	When the user retrieves a case or registry entry, a prompt in the screen panel should indicate whether there are subordinate units which contain screened information. It should be possible to display detailed information according to need, for instance in a separate panel.	O1

8.2.3.4 Temporary blocking of newly registered information

When a new case or document is registered (registry entry, etc.), it is not always clear whether the information should be publicly available or not. This applies in particular to incoming documents (document type I), which are normally registered by the registry office. It is not the task of the registry office to decide what information, if any, should be exempt from public access; this decision usually rests with the manager of the department/section/office or with someone higher up in the hierarchy. Even for documents produced by the organization itself, this matter has not always been decided on when the document is finalized by the executive officer.

In order to prevent sensitive information from becoming known to unauthorized persons before a decision has been made as to its public availability, Noark-4 introduces an automated function for temporarily blocking newly registered information. It is, however, left to the individual organization to decide whether this function is to be implemented or not.

K8.81	The organization should be able to configure a setup whereby all new cases and registry entries (including associated information and documents) which are registered in one or more registry management units, are automatically assigned access code XX, and all information which may be screened using access codes (see K8.60 - K8.65 above) is automatically checked off for screening.	O1

This will result in the information being unavailable to other persons than those authorized to see them, until the XX code is revoked or replaced with another access code.

The authorization for access code XX follows the usual principles. All users should by default be cleared for access code XX. The authorization should normally be limited to cases for which the person is case-responsible and documents for which he/she is executive officer. If somebody is to have access to information which is blocked using access code XX for which he/she is not executive officer (e.g., registry personnel or certain managers), he must be authorized for this access code in the normal way. Managers should normally be authorized for the administrative unit which they head, and registry personnel for the units for which they register. Beyond this, access is restricted according to record-organizational and/or administrative principles as mentioned in K8.53.

K8.82	The temporary blocking of a registry entry should be revoked using a separate command. This command should remove the XX code (it should not be possible to remove the code in any other way) and provide for the assignment of a new access code if the document is to be exempt from public access. It should be possible to revoke the XX code for individual registry entries. However, there should also be a way of revoking the block collectively for all registry entries having the same record date, possibly with a prompt asking whether separate access codes should be registered for individual registry entries. When the XX code is revoked for a registry entry, it is automatically revoked for all associated information as well as for the latest version of all associated documents.	O1

K8.83	When the XX access code is revoked, the attribute *Public access evaluated* (table: *Registry entry*) is automatically filled in with the current date.	O1
K8.84	When the XX access code is revoked for the first registry entry of a case, the XX access code is automatically revoked for the case, too.	O1

Fixed procedures must be established for revoking the temporary block, cfr. 8.3.3 below. To support such procedures, the system should provide for the following:

K8.85	The user should be able to search for cases and documents (registry entries) coded XX which are registered prior to a certain date.	O1
K8.86	The system should have an automated reminder function which makes the user aware of blocked cases/documents which are older than a certain number of days. The organization itself should be able to set the exact number of days.	O1

8.2.3.5 Public access to information - public registry and access to documents

The principle of public access is inherent in the Freedom of Information Act and implies that the general public should have access to the records information and case documents which are not subject to a special provision exempting them from public access in accordance with §§ 5, 5a and 6 of the Freedom of Information Act, cfr. also the regulation, ch. V no. 7. In this context, the general public is primarily represented by journalists. The principle of public access is practised by having public bodies present public registry, and journalists may on the basis of this registry claim access to the actual case documents.

The access control of Noark-4 is designed with a view to enabling the users to fulfil the requirements of the Freedom of Information Act completely. The principles on which it is based, have been presented to the Legislation Department of the Ministry of Justice, who is administratively responsible for the act.

The relations with the principle of public access mainly concern the layout of the public registry. However, provision is also made for processing requests for access to electronic case documents as well as handling external users who are connecting to the Noark base itself.

K8.87	The public registry should be a standard report (to paper or file) according to the description in chapter 11.	O
K8.88	The public registry may also be an export function (electronic). It should contain the same information as the standard report (ch. 11), and it should follow the export format described in paragraph 15.4.2.	O1
K8.89	The public registry should be available in electronic form, as a function in the system.	A

The information to be included in the public registry is based on the Archives Regulation. This is included in the description of the public registry as standard report (ch. 11).

K8.90	In the public registry, registry entries are displayed in chronological order. Information concerning a case is associated with individual registry entries, cfr. ch. 11.	O
K8.91	A public registry, as a report or electronic export function, may potentially include one or more record dates (the attribute *Record date* in the table *Registry entry*).	O
K8.92	If the function for temporary blocking with access code XX is used, a public registry may potentially include the registry entries whose temporary blocking was revoked on one or more dates (the attribute *Public access evaluated*) - see also paragraph 8.3.3 on procedures.	O1
K8.93	Registry entries which are temporarily blocked (access code XX), are excluded from the public registry until the block has been revoked.	O1
K8.94	All registry entries within the dates included in a public registry according to K8.91 or K8.92 which have not been assigned access code XX, should be included in the public registry. Internal documents (types N, X and S) should be handled in the same way as external (types I and U).	O
K8.95	The screening of information in a public registry should be carried out on the basis of access codes according to the following principles: • For registry entires which do not have an access code (i.e., the code is blank), all information included in the registry is displayed, cfr. chapter 11. • For registry entries which have access codes, the information which is checked off according to the principles in K8.60 - K8.62 above, is screened. This means, among other things, that parts of the description of contents will always be displayed in the public registry (see also paragraph 8.3.3 below concerning procedures).	O

Note: *Organizations which resort to temporary blocking using access code XX, should definitely follow the principles in K8.92 and let the public registry include the registry entries whose blocking was revoked on a certain date. This would ensure that all registry entries are included in the public registry, cfr. paragraph 8.3.3 concerning procedures.*

Matters relating to access to case documents should be dealt with by the organization whenever requests for access are received. Even so, it is still permissible, and usually appropriate, to register access codes on electronic documents which contain sensitive information, when the blocking of records information is revoked. This is dealt with in more detail under procedures in paragraph 8.3.3.

As the administration gains experience in electronic recordkeeping and records management, some organizations may want to let external users (journalists and others) search for publicly available information in the Noark base itself. If so, this offer will go beyond what is required by the Freedom of Information Act.

Noark-4 is designed with a view to such opportunities. It is possible to create a separate user type (role) as external user, role 7 - EKS, cfr. K8.9 above. The following particular restrictions apply to read access if a user with role EKS is created:

K8.96	Users having role EKS should only be able to search in and retrieve information which is included in a public registry.	A
K8.97	If the role EKS is defined, there should be a configurable setting which determines whether users with the EKS role may retrieve electronic documents which are not screened, or if retrieval of documents should always require a request for access to information.	A

8.2.3.6 Time limits for screening through access codes

It should be possible to use time limits for the individual access codes to indicate the duration of the screening. This should be a support function to limit the screening in time in accordance with the current laws and regulations. The following functionality is required:

K8.98	For each access code, there should be a time limit. The time limit is registered as the date on which the screening should be (re)evaluated or revoked (the attribute *Date of downgrading*). If the date field is blank, this means that no time limit has been specified.	O
K8.99	It should be possible to fill in the date straight away, or the date may be calculated by the system when the user specifies the number of years.	O1
K8.100	The predefined access codes in Noark should be associated with regular time limits which the system uses for the automatic registration of a date of downgrading for each registry entry. The date is calculated on the basis of *Record date*. The following regular time limits apply: • Codes according to the safety instruction and the security and protection instruction, i.e., the codes **B**, **K**, **H**, **F**, **SF**: 30 years. • Codes which indicate professional secrecy according to § 5a of the Freedom of Information Act, including further specifications, i.e., code **5a** and specialized codes with this statutory authority: 60 years. • Code for temporary blocking, i.e., code **XX**: 14 days. • Other codes: blank.	O

The attribute *Downgrading code* is used to indicate what is going to happen when the specified date is reached. The system should provide functionality for effectuating the downgrading, i.e., revoking the access code based on the downgrading codes.

K8.101	There should be functions for effectuating the downgrading, i.e., revoking the access code for one or more registry entries based on the downgrading code, cfr. the attribute *Downgrading code*. It should be possible to carry out the downgrading using a particular command, either for individual registry entries or for all registry entries which fulfil the criteria, i.e., their date of downgrading has been reached and their downgrading code is either **A** or **S** (cfr. the attribute *Denomination* in the table *Downgrading code*). When a registry entry has been downgraded, the system should automatically set the *downgrading code* to **AU**.	O
K8.102	When a registry entry is downgraded, the system should automatically revoke the access code of associated information and of the latest version of associated documents, provided that their access codes are	O1

	identical to that of the registry entry.	
K8.103	When the first registry entry in a case is downgraded, the access code of the entire case should be revoked, provided that it is identical to that of the registry entry.	O
K8.104	In an enhanced version of Noark-4, it should be possible to have the downgrading effectuated automatically when the date of downgrading is reached. This should be done for registry entries whose *downgrading code* is **S**, but only if the *registry status* is **J** or **A**. Automatic downgrading should be logged, cfr. the table *Additional information*.	O1

8.3 Procedure requirements

Sub-chapter 8.2 describes how the user management and access control must be designed to satisfy the requirements of Noark-4. The administrative procedures required to make these functions work according to plan are described in the following.

8.3.1 User-management procedures

Two kinds of procedures are associated with user management:

- All users, access codes and access groups must be registered in the system. The users must be given rights relating to (authorization for) certain roles, functions in the system and access to information. This is effectuated in one operation when the system is implemented. However, these registrations must be kept up to date. Changes must be made when people quit or are given new tasks, when new people are employed, etc. Changes must also be made when tasks, work routines or the internal organization are modified. It is important that this updating is taken seriously, and that the management considers carefully what roles and rights individuals should have. The quality of the database and the security in connection with the screening of sensitive information depend on this.

- It is necessary to establish procedures which in the best possible way ensure that the individual users maintain their functions in the system according to the intention. This necessitates the establishment and updating of a clearly set-out description of procedures, and the management must follow up the procedures on a regular basis.

8.3.2 Procedures for managing write access

More than before, Noark provides for a number of options with regard to the functionality of the system. There is the option of traditional usage (as in Noark-3), but there is also functionality for advanced electronic case handling and recordkeeping based on the executive officers being assigned extensive rights with regard to registration. The system's provision for such advanced usage does not, however, mean that this is appropriate or advisable in all contexts. This will depend very much on maturity and active preparation. For organizations without adequate procedures and organizational skills, such liberal practice with regard to the executive officers' registration rights may be totally

unjustifiable. In other words, Noark-4 results in greater tension between the options offered by the system and the qualifications of the organizations regarding their use. For most organizations, a major challenge will be to evaluate the usage in the light of current and planned organizational structure and procedures.

In organizations of a certain size, the enhanced registration rights for managers and executive officers require a permanently working apparatus to administer and update the user rights. Likewise, an adequate apparatus is required for follow-up and quality control (registry office). In addition, there is a need for clearly defined and authoritative procedures and executive officers who are well versed in these procedures. It may be sensible to start by introducing electronic case handling with its enhanced registration rights for managers and executive officers in one, or a small selection of, unit(s) within an organization. This allows for concentration, both with regard to training and follow-up of users, and such a scenario with pilot users also makes it easier to gain valuable experience with new procedures.

Neither should the option of having differentiated rights for executive officers on a more permanent basis be ruled out completely. For various reasons, there will always be executive officers with variable training and qualifications for the correct use of the recordkeeping system.

8.3.3 Procedures for managing read access

8.3.3.1 General

In line with the above discussion, the following must be registered before the system can be implemented and changes made to update it:

- any restrictions in the individual users' access to information based on administrative and/or record-organizational criteria (see 8.2.3.1 above)
- access codes used by the organization
- statutory authorities for these access codes (Freedom of Information Act, any additional statutory authority for professional secrecy, etc.)
- clearance of individual users for access codes as well as their authorization for the information screened with these codes
- any fixed access groups
- any members of fixed access groups

Furthermore, a description of what the individual access codes and access groups mean and are to be used for, must be prepared and kept up to date. This material should be easily available to those who use the system, particularly those who perform registration tasks.

8.3.3.2 Revoking temporary blocking

Regular procedures must be established with regard to how the blocking of newly registered cases and case documents/registry entries are revoked. These procedures should, on the one hand, ensure that only authorized persons may revoke the blocking, on the other hand it should ensure that the blocking is not maintained for longer than necessary. The following must be made clear:

- Who is to decide on public access or screening in the individual cases

- Who is authorized to revoke the blocking (authorization in the Noark system)
- Procedures which ensure that the question of public access/screening is dealt with within a reasonable period of time (note that the default time limit for blocking set by the system is 14 days)
- Procedures for communicating between those who make the decision and those who revoke the blocking (if these are different persons)
- Time limit for automated reminder that the blocking has not been revoked, if the system has this function (see 8.2.3.4 above)

8.3.3.3 Producing public registry

Procedures must be established for the printing of public registry, and for the content of the daily version of this registry. It is recommended that one of the following procedures be followed (cfr. the functions for public registry in 8.2.3.5 above):

- If information is temporarily blocked (see 8.2.3.4 above), the public registry is printed at the beginning of the working day and includes all registry entries which were evaluated with a view to public access the day before, i.e., the attribute *Public access evaluated* is filled in with the date of the previous day.
- If temporary blocking of information is not practised, the public registry should include all registry entries which were registered on the same day (e.g., the day before printout), i.e., all that have the same value in the attribute *Record date.*

This should ensure that all registry entires are included in the public registry, and that none of them are included twice.

When parts of the title field on a case or parts of the description of contents on a registry entry are screened (see 8.2.3.3), it is necessary to make sure that the part of the text which is public (available), makes sense without giving away the information to be screened.

8.3.3.4 Processing requests for access to case documents

When requests for access to case documents are forwarded by journalists or other members of the public, the organization must decide on the question of public access on receiving the request. Nevertheless, it will often be necessary to evaluate a case document in relation to the exemption provisions of the Freedom of Information Act even when no request for access to the document has been forwarded. During registration, there will thus be a need for pre-evaluation of the document in order to prevent information which must or should be exempt from public access, from being made known to unauthorized persons at the time of entry into records. This applies in particular to information subject to professional secrecy (§ 5a of the Freedom of Information Act).

The following procedures are recommended in connection with Noark-4:

- Documents which are publicly available, are not assigned an access code in the system. This means the documents may, without further ado, be presented or copied to journalists and other members of the public on request. It also means that such documents in electronic form are openly available to all internal users in the system (possibly excluding some based on administrative or record-organizational criteria, as discussed above).

- Documents which have been evaluated or are to be evaluated with a view to exempting them from public access, are assigned an access code in the system. For such documents, decisions concerning access are made individually when requests for access are received (see, however, the next indent). When such documents are stored electronically, they will also be screened against internal users who are not authorized for the concerned code.
- In line with the opportunities provided by the system, the organization may, in situations where requests for access to a document are likely to appear, consider storing a "public" version of the document where information which is exempt from public access, is left out. The "public" version of the document must then be without an access code, whereas the original version is screened. "Public" document versions which are stored electronically, are identified through a separate version type in the system (see paragraph 5.2.4 above).

8.3.3.5 Registering time limits for screening - revoking access codes, downgrading

It is recommended that default time limits be defined for all access codes for which this is practicable, and that a time limit be defined where blank when cases and registry entries/documents are registered. During registration, it ought to be considered whether screening should apply for a shorter period of time than that of the default value (this does not apply to screening due to professional secrecy according to § 5a of the Freedom of Information Act).

Public bodies should establish regular procedures for revoking access codes when the time limit is reached. This can be done easily by searching periodically for registry entries for which the time limit has expired (see the report in 11.3.6 below), and, if justified, revoking the access code for the registry entry and, if applicable, for its associated case information and case documents.

8.4 Essential tables in the module

Only essential tables have been included here. For a complete overview of the tables in the module and their attributes, see part II, Technical specifications, sub-chapter 14.5.

Table name	Text
Person	Contains all persons in the organization who have rights in the system, as well as all persons to whom the system refers (executive officer, board member, etc.) The identification used for logging on to the system is also stored here.
Person name	Contains the full name of the person as well as his/her official initials as used for registration purposes. A person may be associated with several person names. A separate flag indicates whether this is the person's current name and initials. This is a way to store the history associated with change of name, etc.
Role	Contains information on the rights inherent in a specific role.
Person - role	Associates a person with a specific role. A person may have several

Table name	Text
	roles, one of which must be his/her default role (basic role). The table also associates the person with an administrative unit, registry management unit and records section.
Access code	Contains the access codes which the system uses. Most of the codes are predefined, but it is also permissible to create customized codes.
Clearance for access code	Contains information on the access codes for which a person is cleared. The table has a link to the administrative unit.
Statutory authority for access code	Statutory authority for information exempted from public access, linked to access code.
Access group	Used to store the names of the defined access groups. Access groups are used to limit the access further among the users who are authorized for a specific access code.
Membership in access group	Contains information on the access groups which a person in a specific role is member of.

8.5 Changes from Noark-3 and Koark

The user management and access control is extended and made more flexible than in Noark-3 and Koark. Chapter 16 contains a complete technical specification of the changes and how conversions may be carried out. The most important changes are summarized here:

Basic version (requirement type O):

- The user types have been replaced with roles in Noark-4. Rights and restrictions are associated with the individual roles.
- A person may be registered under several names and initials, and be associated with several roles. This is new.
- The concept of *access code* (attribute) replaces that of *grading code*, cfr. chapter 4.
- A user is (generally) *cleared* for an access code and *authorized* for the code within specific parts of the base. This use of concepts represents a slight change from Noark-3 and Koark.
- Access codes are normally not inherited from one level to another, whereas grading codes normally could be in Noark-3 and Koark.
- A stricter system has been established for indicating the statutory authority of access codes.
- Adjustments have been made as to what information may be screened from public access.
- Screening is carried out by checking off instead of using codes.
- The public registry is more formalized, after a thorough revision (see also chapter 11).

Enhanced version (requirement type O1):

- Rights and restrictions may also be associated with different stages of the handling process, governed by status values in the records management module.

- In addition to the use of access codes, screening may be effectuated through the use of access groups and according to administrative and/or record-organizational criteria.
- An access code for temporarily blocking information which has not been evaluated with regard to public access, has been introduced.
- The downgrading functions have been made more flexible.

9. MODULE FOR BOARD HANDLING

Remains to be translated

10. E-MAIL AND DIGITAL SIGNATURES

10.1 Integration with electronic mail

10.1.1 General

Electronic mail (e-mail) was originally meant as a tool for exchanging electronic notes and documents between personal mail boxes. For public-administration bodies, it may also be of interest to use e-mail for the development of case documents. However, satisfactory technical solutions which maintain the formal document requirements of public administration, have not been implemented in current e-mail systems. In 1995, the Ministry of Government Administration prepared a special guide focusing on issues relating to public access, registration (entry into records) and filing[7]. Case documents should be registered and filed, even when they are distributed electronically. Public-administration bodies which dispatch or receive case documents by e-mail, must therefore implement a system and set of procedures which ensure that the documents are entered into records and filed in the same way as incoming and outgoing case documents in paper form.

NOSIP[8] requires that e-mail systems used by the state administrative bodies should have certain qualities in accordance with the international X.400 standard. X.400 systems have receipt functions, but otherwise these systems are not adapted to document exchange between administrations. X.400 systems have also proved to be on the decline in the market. At the same time, functionality has been added to Internet-based (SMTP/MIME-based) and proprietary e-mail systems. Public-administration bodies must at any rate be able to exchange e-mail with other systems than those based on X.400.

The e-mail systems do not have built-in functionality for maintaining the *mail-handling* rules of the state administration. Thus, each organization must establish procedures for this. General specifications for handling the dispatch and receipt of case documents as e-mail have been drawn up as part of the Statskonsult program "Nasjonal infrastruktur for EDB" [National infrastructure for computer-based processing][9]. These specifications acknowledge the important distinction between case documents which are authorized and dispatched on behalf of an administration, and other documents of a more informational or

[7] «Bruk av elektronisk post (e-post) i statsforvaltningen» [«The use of electronic mail in the state administration»] (Ministry of Government Administration, December 1995).

See also «Elektronisk post i statsforvaltningen» [«Electronic mail in the state administration»]. Enquiry from a workgroup appointed by the Ministry of Government Administration. Presented 9.6.1995.

[8] NOSIP-2.0 - Norsk OSI profil. Statskonsult [the Directorate of Public Management], 1996.

[9] «Retningslinjer for allokering av nettadresser (NSAP-adresser) og adresser for elektronisk post (O/R-adresser) innen offentlig forvaltning» [«Guidelines for the allocation of network addresses (NSAP addresses) and addresses for electronic mail (O/R addresses) within public administration»]. Report 2.9-10 (20.05.1992). Statskonsult, 1992.

private character. The specifications assume that official e-mail receptions will be established in each organization to handle ordinary case documents exchanged as e-mail. The mail reception must be associated with the registry office of the organization. Based on the solution with centralized mail receptions, the following rules for mail routing (means and route of dispatch) have been specified:

1. Institutionally addressed e-mail should be routed to the centralized e-mail reception of the addressee, which presumably is localized in, or in connection with, the registry office of the organization.
2. Mail should also be addressed and routed to this centralized mail reception when the executive officer is specified as secondary addressee (institutionally addressed mail with «attention» for personal addressee). In such a case, a copy should automatically be forwarded to the (personal) mailbox of the executive officer.
3. Personally addressed mail should go straight to the personal mailbox of the addressee without being entered into the records.

A Noark system *should* include integrated functions for the registration of e-mail as well as for the dispatch and receipt of case documents based on a centralized mail reception. However, case documents and other documents of archival value received by e-mail *must* be registered (entered into records) and filed even if such integrated functions are not available. The duty to register case documents applies irrespective of whether the document is sent to a centralized mail reception or to a personal addressee.

The following principles are recommended for the use of e-mail when dispatching case documents:

- An e-mail system with good *receipt mechanisms* is very useful in that it makes it possible to follow up and check if the mail has been received and read. If the e-mail system has such mechanisms, receipt for *delivery*, and preferably also for *opening/reading*, *must* be enabled during all dispatches of case documents.
- A person who dispatches a document by e-mail, is responsible for checking that the document arrives - by checking that a delivery receipt is returned or by other means.
- Before e-mail is used, it must be established that the addressee accepts the use of e-mail and checks regularly if e-mail has been received. Receiving an incoming case document by e-mail from an external organization is considered as accepting the use of e-mail for reply.
- An authorized archival format *should* be used for the dispatch of the main document and attachments, since this is a format which all addressees are presumably able to read. Other formats *may* be used, provided such use is cleared with the addressee in advance.
- The same applies to the use of digital signatures and any encryption. It is necessary to make sure in advance that the addressee is able to handle the format to be used.

Case documents *should* be sent using dedicated functions in the case handling system or Noark system which as far as possible simplify both the registration (entry into records) and the dispatch itself. Likewise, registry personnel, and possibly also the executive officer, *should* have access to functions which simplify the registration and filing of case documents received by e-mail. In the following, this is referred to as integrated use of e-mail, and the functional requirements relating to it are specified in 10.1.3.

The use of an independent e-mail system where there is no kind of connection with the Noark system, is referred to as non-integrated use of e-mail in the following. No functional requirements apply, but some issues relating to the establishment of procedures, etc., are discussed in 10.1.2.

10.1.2 Non-integrated use of e-mail

Organizations which use e-mail that is not integrated with the Noark system, must establish procedures to ensure that case documents which executive officers receive, are forwarded to the registry office for registration and filing.

Procedures must also be established for outgoing e-mail. The following three options apply:

1. The executive officer forwards the document to the registry office for registration and dispatch.
2. The executive officer registers and finalizes the letter himself/herself in the Noark system before dispatching it.
3. The executive officer dispatches the document and forwards a copy to the registry office for registration.

If it is possible to add customized functions to the e-mail system, a function for forwarding to the registry office should be added.

If the e-mail system permits, another option is to prompt the user automatically as to whether the document should be forwarded to the registry office for filing when a message with attachments is sent to recipients within the organization. For incoming e-mail, this kind of functionality may be used to prompt about forwarding to the registry office after the user has read an e-mail which meets certain criteria (the most typical being that the e-mail is *external*).

If the e-mail system permits no such customization, or if the regular use of control questions is not desirable, a denomination for the e-mail address of the registry office to be used for forwarding should be added.

Case documents sent by e-mail should normally have the e-mail address of the organization as sender. Replies will then be sent straight to the mail reception unless the sender explicitly specifies the executive officer as addressee. Most e-mail systems have no option for specifying a different sender from the one who carries out the dispatch. Procedures should therefore be established to ensure that executive officers indicate that reply should be sent to the e-mail address of the organization.

Other measures to encourage the use of the e-mail address of the organization for the dispatch of case documents are the following:

- The e-mail address of the organization is specified in all document templates, letterheads, business cards, printed matter, etc.
- Personal e-mail addresses are used on business cards, etc., only when the official address of the organization is also specified.
- Specific procedure descriptions are drawn up to distinguish between informal e-mail which is not to be registered, and e-mail to be registered and filed.

- Procedure descriptions are drawn up to ensure that clients are always informed that formal enquiries are to be sent to the e-mail address of the organization, even in cases where an employee has found it necessary to specify his/her own personal e-mail address.

10.1.3 Integrated use of e-mail

The integrated use of e-mail will simplify the tasks of executive officers and registry personnel.

When an executive officer (or manager) dispatches case documents by e-mail using the functions of the Noark system (preferably made available from the case handling system), the necessary registration in the mail registry is automatically carried out. The task of the registry personnel may in such cases be limited to controlling the quality of the registration, and possibly to converting case documents into an archival format.

The fact that executive officers are able to dispatch electronic documents in this way should not stop those who wish to from letting registry personnel carry out the dispatch. Thus, the registry personnel must have access to functions which enable them to dispatch on behalf of any executive officer.

In a Noark-system, there should be functions which simplify the registration and dispatch by registry personnel of case documents received by e-mail. Such functions may be useful when new registry entries are created, as well as any case entries, and when electronic documents are transferred to document storage.

Since a considerable proportion of the case documents which are received by e-mail, must be expected to be sent straight to the individual executive officers rather than to the mail reception of the organization, it is recommended that executive officers be given access to the Noark function for registering and filing incoming e-mail. Such a well-integrated registration function where an executive officer only has to specify a small amount of information beyond that given by the message, may contribute considerably to ensuring that case documents which are sent straight to executive officers, are registered.

10.1.3.1 Noark head

For e-mail which includes case documents, Noark has specified a separate attachment with records information. This should provide for a more automated exchange of records information between two organizations which both use Noark systems. In the following, this e-mail attachment with records information is referred to as the Noark head.

The structure of the Noark head is based on SGML syntax. As a minimum, it should contain the name of the sender (organization), case title, case and document number, date and description of contents for the letter as well as a unique reference to the registry entry. Beyond this, it should be possible to enhance the head with attributes according to the needs of the organization.

The detailed technical requirements for the Noark head are described in sub-chapter 15.2.

The exchange of a Noark head with the case documents has the following advantages:

- The sender is identified to the addressee.

  This may contribute to increased security in connection with the dispatch of case documents between administrative bodies.

- Automated registration for the addressee.

  This is based on essential records information from the sender system contained in the Noark head. In later correspondence with the same sender concerning the same case, the Noark head will be able to return the necessary reference codes (case number, etc.) to effectively - possibly automatically - perform the registration in the Noark system of that organization.

Sub-chapter 15.2 specifies the format of the Noark head, but it is up to the individual vendors to design solutions for integrating and importing records information from the Noark head. To what extent such information should be checked and verified by the registry office of the addressee, will depend on the kind of quality-control functions the addressee chooses to implement. Irrespective of this, the registration function for incoming mail will be rationalized. In a fully developed system, one may realistically envisage fully automated registration of case documents between clients who have authorized each other for this purpose.

Such streamlined dispatch and registration of case documents may make it less tempting for executive officers to send case documents by e-mail without using the integrated functions.

10.1.3.2 Formalized functional requirements for the dispatch of e-mail

K10.1	The dispatch of case documents with e-mail should be integrated in Noark as a function in the records management module.	E
K10.2	The Noark function for the dispatch of case documents with e-mail should be available to executive officers.	E1
K10.3	Only case documents which have been finalized by the executive officer, may be dispatched by e-mail.	E
K10.4	It should be possible to dispatch the document simultaneously to all addressees registered in the registry entry where the e-mail address is specified.	E1
K10.5	If no e-mail address is registered in the registry for one or more addressees, the system should permit the user to specify their addresses as part of the dispatch. The system should in such a situation also update the registry with these e-mail addresses.	E1
K10.6	There should be a function which provides a summary of recipients (addressees) where the document is not sent by e-mail, or where the e-mail failed.	E
K10.7	When case documents are dispatched, it should be possible to attach a Noark head which fulfils the requirements described in sub-chapter 15.2.	E1
K10.8	A dispatch of case documents should be complete, i.e., it should contain the main document and all attachments. If one or more attachments exist only in paper form, the main document *should not* be dispatched by e-mail. Note that this should not prevent an *informal* dispatch of the documents which exist in electronic form.	E
K10.9	It should be possible to choose whether the archival format or the	E

	production format should be used for the dispatch. The archival format is the default if the document exists in this format.	
K10.10	When the Noark head is used, it should be possible to register information about selected clients' use of document formats and their accepting digital signatures and encryption. It should be possible to enter the information in a separate register (see 14.2.28-29).	E1
K10.11	When e-mail is sent, it should be checked against this registry. If documents and/or the use of a digital signature do not correspond to registry information on the addressee, it should be possible to cancel the dispatch.	E1
K10.12	The default value for the subject field of the message should be the *description of contents* from the registry entry, screened for any information which is exempt from public access. It must be possible for the sender to modify the subject field.	A
K10.13	The e-mail address of the sender should normally be the address of the e-mail reception of the organization, regardless of who carries out the dispatch.	A
K10.14	It should be possible to connect to and use a system for digital signatures based on public key cryptography. It should be possible to apply a digital signature to the entire dispatch (main document, attachments and, if appropriate, the Noark head) to guarantee the integrity and authenticity of the dispatch. In addition, it should be possible to apply digital signatures to the individual documents which make up the dispatch, in order to authorize the document contents, instead of using a hand-written signature.	E1
K10.15	It should be possible to use a connected system for public key cryptography for encrypting documents for dispatch. For documents which are subject to exemption from public access, encryption is a prerequisite for the use of e-mail.	E1
K10.16	For each recipient (addressee) of a document dispatched by e-mail, the system should add a record in the table *Additional information* associated with the registry entry. This additional information should include the name and e-mail address of the addressee, dispatch time and who sent the document.	E
K10.17	For each addressee to whom the case document is dispatched by e-mail, the *Dispatch status* in the addressee record should be set to S (Sent), cfr. paragraph 14.2.17.	E
K10.18	The system should have a function for automatically transferring a receipt from the e-mail system (delivered, opened/read, failed) to the attribute *Dispatch status* in the addressee record.	E1
K10.19	For the individual access code, it should be possible to specify whether the dispatch by e-mail of a document which is protected by the access code, should be permitted, and if so, whether encryption is necessary.	E
K10.20	To prevent a document which contains information subject to professional secrecy, from being dispatched by e-mail to unauthorized persons, there should be an option in the address list for indicating to what clients the document may be dispatched. It should be possible to	E1

	specify what access codes the individual person is authorized for, as well as the time interval for which the authorization applies.	
K10.21	The system should not permit documents to be dispatched in conflict with the limitations imposed by the access code and the authorization of the addressee for that code. If such a function exists, it should be possible to disable it for individual users or for all users.	E1

10.1.3.3 Formalized functional requirements for registering received e-mail

K10.22	A function for importing case documents received by e-mail should be available in the records management module of Noark.	E
K10.23	Only registry personnel should be allowed to register incoming mail (enter it into the records) specifying a different person from himself/herself as executive officer.	E
K10.24	The inbox of the e-mail system should be accessible as part of the Noark system, so that documents to be registered/filed may be selected straight from the inbox without having to be exported from the e-mail system first.	E1
K10.25	In order to provide optimal support for the registration (entry into records), the Noark system should, in a clear way, present information from the document which is selected in the inbox. This should include relevant information from the e-mail system as well as from the Noark head, if included in the message.	E
K10.26	The system should have an option for viewing the attachments to the messages (e.g., using a "viewer").	A
K10.27	If the Noark head contains references to an existing case, the Noark system should retrieve that case automatically and offer registration under it. This should not prevent the user from finding another case under which to register the letter.	E1
K10.28	It should be possible to create a new case as part of the registration of an incoming e-mail. It should be possible to use information from the e-mail system as well as from any Noark head when the case is registered.	E
K10.29	When a registry entry is registered, it should be possible to choose what parts of the information from the Noark head and the e-mail are to be used. It should be possible to file the e-mail linked as a *dispatch letter* to the case document in question, or possibly as the main document of the registry entry.	E
K10.30	If the message contains several attachments, the user should be able to select which one is to be registered and filed as main document, and what are to be attachments or other kinds of additional documents.	E
K10.31	If the registration is not carried out by registry personnel, the person who performs the registration should be specified as executive officer, and possibly as case-responsible if a new case is created.	E
K10.32	Registry status should be set to S and document status to F when somebody other than registry personnel registers. Registry personnel	E

	should be able to select registry status.	
K10.33	It should be possible to provide for the automatic registration of e-mail from selected clients when the message includes a Noark head.	E1
K10.34	The Noark function for registering and filing case documents received by e-mail should also be available in the case handling system for executive officers who are authorized for such registration.	S1
K10.35	In the case handling system, there should be a function for forwarding received e-mail to the mail reception for registration and filing. This function should enable executive officers to enter additional information which may be useful to registry personnel during registration.	S1

10.2 Using digital signatures and encryption

10.2.1 The uses of digital signatures in Noark

A Noark-based system should be able to handle the use of digital signatures for two different purposes:

- to confirm the authenticity of the sender and maintain the integrity of documents during dispatch and filing
- to authorize the contents of documents, as a replacement for a hand-written signature

Noark must thus provide for the use and management of digital signatures in two different contexts:

1. when (external) documents are sent and received
2. when documents are filed

Normally, procedures for the use of digital signatures in connection with the *internal* document flow are not provided for. The need for internal authentication is considered to be sufficiently attended to by Noark's automated registration of person(s) responsible for performing key activities as well as system functions for activity logging. The system does, however, have an option for applying digital signatures to document versions as part of the internal processing.

10.2.2 Use in connection with dispatch and receipt

To authenticate a *dispatch*, it is considered sufficient to use the digital signature of the organization (registry office) on all documents.

To authorize the *document contents*, however, it must be possible to apply one or more personal digital signatures to the individual documents to be authorized.

It is also possible to use a personal signature to authenticate the dispatch, and thus to enable the dispatch of documents without the digital signature of the organization being added by another office.

An addressee must be able to verify signatures, whether they belong to the organization or to individuals. The certificate will normally be sent together with the signature, which simplifies the verification process. The certificate is presumably filed locally in connection with the received document. The validity of the certificate at receipt time is checked against the relevant TTP service (Trusted Third Party).

The lookup against a TTP is presumably performed in a more or less automated way. The manner in which the verification is performed, is considered to be outside the scope of Noark. This also applies to the unresolved issues concerning the ability of TTP services to verify certificates on a long-term basis.

The primary task in a Noark context will be to handle the verification and any checking of the certificate against TTP during receipt. Later verification of the same signatures may be performed against the locally filed certificates, which have previously been verified against TTP.

10.2.3 Use in connection with filing

A digital signature is always associated with the format of the document at the time when the signature was applied. Converting the document from this format to an archival format breaks the bond between the document and the signature. Thenceforward the digital signature can no longer be used to authenticate or guarantee the integrity of the filed document.

A digital signature applied by the sender in a production format is, in other words, destroyed when the document is converted to an archival format. If the use of a digital signature is desired for filing after such conversion, a new signature must be applied after the conversion process. The signing may use a secret key associated with the mail reception of the organization, or the person who performs the conversion may apply his/her own signature. The latter option is normally preferable.

"Archival signing" of a received document during conversion to archival format should be performed only after the result (contents) has been checked against the original. If it is desirable to preserve traces after the verification of digitally applied signature(s), one could let the new archival signature include the result of the verification process. *In addition*, the document may be stored digitally signed in the form in which it was received (i.e., in the production format of the sender), so that the converted archival version may be compared with the original as long as the latter is readable.

10.2.4 Encryption

From the Noark point of view, all encryption should take place outside the recordkeeping system, but in a couple of areas it is still necessary to formulate Noark requirements in order to avoid losing documents of archival value because they cannot be decrypted after they have been transferred to archival repository.

Encryption is most likely to be used for the exchange of documents. This presupposes that the document is decrypted before being filed, irrespective of whether public key cryptography (asymmetric encryption) or another encryption method has been used.

Another prospective area for the use of encryption is the storing of electronic documents in a document storage. In order to prevent the access to documents from depending on individuals, the use of personal encryption keys is not permitted for filed documents. This

applies irrespective of whether the method is based on symmetric or asymmetric encryption. It is also irrespective of whether the encryption key must be stated explicitly by the user, or if it is implicit in a password used for logging on (PIN code, etc.).

10.2.5 Formalized functional requirements

K10.36	The Noark system should offer functionality for handling digital signatures based on public key cryptography.	E1
K10.37	There should be a function for applying to a document one or more digital signatures in order to authorize the contents of the document. It should be possible for the executive officer, as well as any other person who is to sign the document, to use this function.	E1
K10.38	Digital signatures applied to filed case documents should be stored in a separate table, *Digital signatures*. Detailed requirements concerning this table are described in chapter 14, Modules, tables and attributes.	E1
K10.39	It should be possible to file a signed document in the original format with all signatures included. If used, such a format should complement (not replace) the archival and production formats.	A
K10.40	There should be a function for verifying digital signatures. It should be possible to store status information from the verification process in the table *Digital signatures* together with, or instead of, the signature that is verified.	E1
K10.41	It should be possible to store certificates associated with the help index for clients. This may be done by storing the certificates themselves in the help index, or by having the help index include a reference to externally stored certificates.	E1
K10.42	There should be a function for checking the validity of certificates used for verifying digital signatures against TTP.	E1
K10.43	When a dispatch or document is given a digital signature, and possibly also encrypted, the Noark system should guide the user through the process of decrypting and verifying the signature. This process should include all signatures used. It should offer the user to check the certificate against TTP, and should be able to perform automatic checking against locally stored certificates. It should not be obligatory to check a certificate against TTP.	A
K10.44	When a document is given a digital signature, it should automatically be blocked against changes.	E1
K10.45	It should not be possible to apply a digital signature to a document after the document has been marked as finalized by the executive officer/manager. This should not preclude the possibility of signing an e-mail in which the document is included.	E1
K10.46	It should be possible to apply several digital signatures to the same document.	A
K10.47	It should be possible to let a digital signature include only the document, or the document as well as previously applied digital	A

	signatures.	
K10.48	It should not be permitted to file signatures applied to outgoing e-mail in order to authenticate and guarantee the integrity of a dispatch (in other words, not a single document).	E1
K10.49	The system should be able to file status information from the verification of signatures which a sender has applied to received e-mail. Information on the verification should be filed with a link to the main document of the dispatch. The system should not permit the filing of the signature itself if it includes more than the main document.	E1
K10.50	When a received document is converted to archival format, it should be possible, but not obligatory, to apply a digital signature to the document as a token that the converted document has been checked against the production format and its contents found to be identical.	A
K10.51	During signing in connection with conversion to archival format (see above), it should be possible to let the signature include any verification of signatures on the original in order to associate these with the converted document.	A
K10.52	It should not be permitted to use personal encryption keys when documents are stored in archival format.	E1
K10.53	When documents are transferred to archival repository, no documents should be encrypted. Exemptions from this provision may be granted for particularly sensitive material with prior arrangement.	E1

11. REPORTS

Not translated

12. PERIODIZATION, REMOTE STORAGE AND TRANSFER TO ARCHIVAL REPOSITORY

12.1 Purpose

As part of the recordkeeping and case handling functions of an organization, the Noark base and physical records continuously have new registrations and documents added to them. The volume increases, and most of the information and documents will be of less interest as time goes by. This is the basis for periodization, remote storage and transfer to archival repository. These functions apply to both physical records and the Noark base.

Remote storage means that the oldest material, which is no longer used extensively, is stored in an appropriate place (remote-storage records), while the most recent material is kept easily accessible for daily use (active records). Throughout the years, a number of different principles have been employed, many of which have not been particularly successful. The major problems have been

- vague criteria with regard to what is subject to remote storage, leading to doubts as to whether a case is to be found in the active records or the remote-storage records
- lack of system in the remote storage, upsetting the original system of the records during transfer to remote-storage records. This reduces the chances of retrieval

When the Noark standard was introduced from 1984 onwards, a system of regular *registry periods* (or records periods) was established as a standardized solution for the state administration. Put simply, this has the following consequences:

- All cases containing documents which have been registered within a specific time interval, for instance a five-year period, are transferred to remote storage simultaneously and constitute a unit in the remote-storage records.
- All registrations in the Noark base within the same time interval are taken out of the active Noark base and entered into a historic base and/or preserved as printouts on paper or microfiche.

This kind of periodization has been very successful in that there are definite criteria for what is subject to remote storage, and the remote-storage records are systematic and easily retrievable. The principle of having regular remote-storage intervals is appropriate for topic-sorted and generally case-oriented records. For object-sorted records material, however, such as personnel files, client files, property files, etc., such a regular division may occasionally be somewhat impractical. It may be more appropriate to use a different remote-storage principle from one that uses regular time intervals for everything. For instance, one might want to keep the personnel file in the active records as long as a person is employed by the organization, whereas the file may safely be stored in a remote location when the employee leaves. It has also proved difficult to find appropriate solutions for handling records in connection with reorganizations which involve the moving, merging or splitting up of organizational units.

Noark-4 maintains the principle of regular registry periods, but incorporates more flexibility in the remote-storage principles. This should address various needs for various types of records material while making it easier to handle records material in connection with certain kinds of reorganizations. Increased flexibility requires better tracking, and it is therefore provided for the Noark base to keep track of the different principles for remote storage of records. The solution should also make it easier to implement new filing plans, etc.

However, it is not possible to prescribe solutions which are appropriate for all kinds of reorganizations. Such changes occur in many different guises, and each case has to be considered separately.

The principles for remote storage and periodization are based on the Noark records management function keeping track of and controlling the physical records (on paper). The same principles may, however, be employed to great effect for electronic records. The difference is mainly that electronic records are an integrated part of the Noark base, which means that the structure and periodization of the records automatically follow the same principles as the records management system, i.e., no particular intervention is needed for the records.

Transfer to archival repository is meant to relieve the originating organization (records creator) of older records material and provide for the serving of users interested in the material (researchers, etc.). The transfer is based on the structure of the remote-storage records, and its quality will thus be essential to the subsequent use of the material.

12.2 Principles and functions

The functionality of periodization and remote storage in Noark-4 is based on the following main principles:

- A system of clearly defined *records periods* which apply to both physical (paper) and electronic records. Records periods should generally be the same for all records sections within the same *records entity* (see ch. 7), but this is no absolute requirement. The length of the periods (or intervals) are fixed by the organization itself, but they should always be an entire number of years, and the use of shorter periods than 4-5 years is not recommended. All periods do not have to be of the same length, although that does make it easier to keep track.
- The principles for the remote storage of records are decided individually for each records section. The division of the records into records sections should therefore take into account any need to differentiate the remote-storage principles.
- In records sections which are topic-sorted, *all cases* which are *finalized* during the records period, are stored in a remote location. The remote storage is usually carried out two years after the end of the records period. This makes it possible to single out cases which are to continue into the next records period. The functions and procedures are described in more detail in 12.3.1.

- In records sections which are object-sorted, all *objects* which are deemed to be of no current interest at the end of a records period, are stored in a remote location (for instance, a personnel file for an employee who has left during the records period). Objects for remote storage may be singled out gradually during the period, but the remote storage itself is carried out at the end of the period, preferably simultaneously with the remote storage of the topic-sorted records sections.

  If the objects are of a type which will "always" be of current interest (such as farm-number in a district council), it is recommended that the same remote-storage principle be used as for topic-sorted records sections. In this case, however, the remote storage should be postponed until the cases in question are of little interest, for instance by keeping the last two periods in the active records while storing the third-last period in a remote location. The functions and procedures for the remote storage of object-sorted records sections are described in more detail in 12.3.2.

- In records sections which are sorted according to board meeting (minutes, any summons, case plans, etc.), remote storage is carried out for *all meetings* which are *held* during the records period. The functions and procedures are described in more detail in 12.3.3.

- Registrations for terminated records periods are kept in the active Noark base as long as appropriate, i.e., as long as there is a need for speedy access to the information, and as long as this does not create problems in terms of the size of the base. For paper-based records, this means that the active Noark base may refer to records sections which are to be found in remote-storage records entities. For electronic records, it means that the documents from terminated periods may still be in the active base.

- When the Noark base is reorganized, i.e., when information and any documents from terminated periods are removed from the base, this applies to one or more *entire* records periods. It should not be possible to remove registrations and documents which are associated with active records sections, from the base. This means that cases associated with objects which are of interest for a long period of time, may remain in the active base for several records periods. Registrations and documents which are removed from the active base, are stored in one or more historic bases and kept there until being transferred to archival repository. The reorganization of Noark bases is described in more detail in 12.3.4.

The functions for periodization of the Noark base and for controlling the remote storage of the physical records are mainly associated with the table *Records section* in the record-structure module. The following requirements apply to the system:

K12.1	It should be possible to indicate the remote-storage principle of a records section by means of a formalized code and en explanatory text, cfr. the table *Remote-storage code*. Topic-sorted records sections should have a remote-storage code for regular periodization (code F) as default, but it should be possible to modify the value.	O
K12.2	For individual records sections, it should be possible to register a records status with a fixed set of values. The permissible values are specified in the table *Records status.* The values for records status should control the registration options as indicated in K12.3-K12.6.	O
K12.3	The value A (active) should keep the records section open to all kinds of registration.	O

K12.4	The value O (overlap period) should keep the records section blocked against the registration of new cases, but open to the registration of new documents. When new documents are registered in a case which belongs to a records section having this status, the entire case should automatically be transferred to the *successor* of the records section, cfr. K12.7 below. The user should be made aware that the case is transferred to a new records section, and be prompted to move the case in the physical records (unless the document is stored electronically). If the sorting principle (filing plan) at the successor is different from that of the predecessor, the user should be prompted to change the filing plan code on the (paper) document.	O
K12.5	The value U («uaktuell», i.e., of no current interest) should lead to the records section being blocked (closed) against all kinds of registrations. However, it should still be permissible to move a case or a group of cases (in its entirety) to or from a records section having status U. The system should only allow the move if the two records sections have the same sorting principle.	O
K12.6	The value B («bortsatt», i.e., stored in a remote location) should lead to the records section being blocked against all kinds og registrations. It should nevertheless be permissible to move a case or a group of cases (in its entirety) from another records section to a records section having status B. In such situations, the system should check that the two records sections have the same sorting principle.	O
K12.7	A records section having status O should always refer to a successor which constitutes the corresponding records section in the next records period. It should also be possible for records sections having status B or U to refer to a successor.	O
K12.8	Records sections should be identifiable through a unique number, and it should be possible to associate the individual records sections with a records period by referring to the number of the period.	O
K12.9	All records sections should have a start date registered. Records sections having status B should also have an end date registered.	O
K12.10	It should be possible to register a physical address for all records sections.	O
K12.11	It should be possible to register notes on all records sections.	O

Using the functionality described above, the periodization may be represented as a structure in the Noark base. When the base is to be divided according to this structure, i.e., the Noark base is reorganized, functions for data export and the controlled deletion of information from the base are required. The following requirements apply:

K12.12	The system should be able to export data from the base in accordance with the export format specified in chapter 15. The export function should be able to handle all the attributes which according to chapter 14 should be included during export, and which have been implemented in the system. The export function should, furthermore, be able to include any additional information in accordance with K3.50.	O
K12.13	It should be possible to export freely selected parts of the base, such as a records section, cases created during a specific time interval, etc.	A
K12.14	There should be a standardized function for exporting *records periods*	O

	from a Noark base. This function should comply with the requirements of K12.15-K12.16.	
K12.15	It should be possible to export one or more *entire records sections* as specified by the user. This export includes both registrations and electronic records (if present in the base). The system should flag which records sections are exported using the standardized function. The user should be able to reset these flags with a view to re-running the export job.	O
K12.16	In addition to the cases included in the specified records sections (K12.15), it should be possible to have the export include cases from other records sections whose record date is within the specified period. For these cases, a *copy* of the following is exported: • all case information • the value in *records section* is kept unchanged, indicating which records section the case now belongs to • the value in *case status* is changed to KU ("kopiert utdrag", i.e., copied excerpt) • all registry entries whose record date is within the specified period, including their associated information (this normally means that only some of the registry entries within a case are included) • for electronic records (requirement type O2) only: all electronic documents associated with the included registry entries The record sections subject to such copying should not be flagged for completed export.	O
K12.17	The system should be able to delete entire records sections from the base. It should only be possible to delete records sections which are flagged for completed export.	O
K12.18	The system should be able to import data from the export format of a Noark base. This import may include all the attributes which according to K12.12 should be exportable.	O
K12.19	The system should furthermore be able to export and import all attributes which are not obligatory for export/import.	A
K12.20	During export, the system should include an attribute which identifies the base from which the export has been made. During import, this attribute should be stored in the base to which data are imported. The format should comply with the specifications of EI.BASEID in paragraph 15.2.2.1, cfr. K10.7.	O1
K12.21	A Noark system should be able to operate on several records data bases in parallel. The bases are distinguished from each other through the attribute for base identification, cfr. K12.19 above. The base identification should provide for uniqueness in cases of overlapping between the number series of different bases.	A
K12.22	If a physical division within cases is used (see K7.17), it should be possible to move records sections to other records sections, exactly as for entire cases according to K12.5 and K12.6. This is an obligatory requirement if K7.17 is implemented.	A
K12.23	If a physical division within cases is used (see K7.17), the system should provide for case sections associated with a records section exported according to K12.15, to be exported in a similar manner to that of entire cases within the records section. If the cases concerned belong	A

	to a records section which is included in the export, no particular action is necessary. If, on the other hand, the cases are not included in the export in their entirety, the export should include a *copy* of the following from the cases concerned: • all case information • the value in *case status* is changed to SD («saksdel», i.e., case section) • all registry entries included in the case section • for electronic records (requirement type O2) only: all electronic documents associated with the included registry entries This is an obligatory requirement if K7.17 is implemented.	

12.3 Procedures and routines

The procedures for periodization, remote storage and transfer to archival repository determine the subsequent quality of the records. It is therefore important to implement them securely and accurately, and to document them well. It is recommended that the following procedures and routines be strictly followed, and any deviations deemed necessary should be thoroughly evaluated, planned and documented. If special conditions apply to a records section, such as the transfer of the material to another organization, the note field in the table *Records section* should be used to account for this.

It is also important to be familiar with rules and regulations concerning remote storage and transfer to archival repository. The state administration has had such rules for a number of years, and similar rules are likely to be introduced for local and regional administrations when the new Archives Act enters into force. Individual repository institutions are also likely to make demands in connection with the transfer.

In view of this, one is generally recommended to contact the repository institution to which the transfer is to be made, for the drawing up of remote-storage procedures as well as for the reorganization of a Noark base.

12.3.1 Remote storage of a topic-sorted records entity

The remote storage of a topic-sorted records entity, i.e., the records sections using a topic-based sorting principle, follow the division into records periods. All cases which are finalized within the records period in question, are stored simultaneously.

To make the transition between two records periods fit in as smoothly as possible with the daily routines, it is recommended that the first two years of each new records period be defined as *overlap period*. As the name suggests, this is to be regarded as a transitional phase between the old period and the new one. The overlap period is used to clarify which cases are still active and should thus continue into the new records period, and which have been finalized and thus belong to the terminated period.

At the end of the overlap period, it is time to take stock and carry out remote storage. The active cases (belonging to the new period) are those which have been created during the overlap period as well as those older cases to which new documents have been added

during the overlap period. Finalized cases (belonging to the terminated period) are those which have not been active during the overlap period. Depreciation of any non-depreciated documents in these cases is carried out, whereafter remote storage is carried out for all cases which belong to the terminated period.

Figure 12-1 shows the overlap periods in relation to the records periods and the time of remote storage.

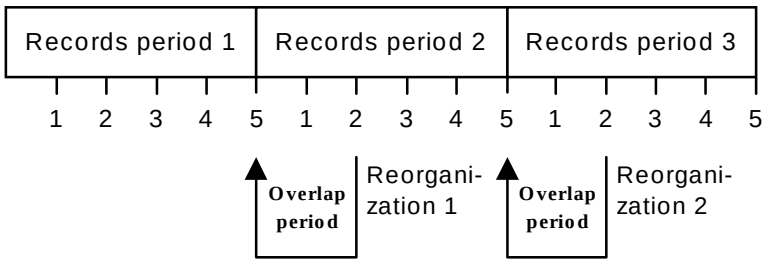


Figure 12-1: Use of overlap periods for periodization

The following procedure is recommended for periodization and remote storage:

- At the beginning of the overlap period, records status is set to O for the records sections where a period division is envisaged. This means that these records sections are automatically blocked against any registration of new cases. At the same time, new records sections having status A are being created. These are registered as successors to those with status O. The same records section may, if desired, be registered as successor to several records sections.
- In the physical records, separate files are created for the new period, so that it is possible to distinguish between the cases of the new and old periods. The two sets of files are kept in separate records entities for the duration of the overlap period.
- In electronic records, no particular action is required. The division into records sections follows automatically from the registrations in the records management system.
- Cases which are new and documents which are subsequently registered in these are always associated with a records section having status A.
- When a new document is registered in a case from the old period, i.e., in a records section having status O, the entire case is automatically moved to the succeeding records section, and the system prompts the user. The user must make sure the case is moved into the new physical file for the new period, and must, if applicable, change the filing plan code if the sorting principle (filing plan) has been changed compared to the old period (cfr. the prompt from the system). The relation between the successor and the predecessor should make it easy to determine which records section the case has been transferred from.
- At the end of the overlap period, it must be checked whether all cases which still belong to records sections having status O (i.e., the old period), have been finalized, i.e., having *case status* = A (or, if the attribute *Case status* is not used actively, whether all registry entries in these cases have been depreciated). Should there be any cases which have not been finalized and are non-finalizable after two years of passiveness, the case should be transferred to the successor. Active precedent cases, i.e., precedent cases for which the

precedent has not been revoked, are transferred to the successor. After this, the status of the terminated records section is changed from O to B, and the physical records for the period is stored away (if the procedure recommended above has been followed, it already constitutes a separate unit). The section for remote storage is blocked against any new registrations.

- Remote storage of finalized records sections (periods) in electronic records is part of the procedures for the reorganization of the Noark base, cfr. 12.3.4 below.

If an overlap period is used and the above procedure followed, the following cases should continue into the new records period:

- Cases which have been created during the overlap period, i.e., after the period division
- Cases from the previous period to which new documents have been added during the overlap period
- Active precedent cases (i.e., from which the precedent has not been revoked) from the previous period
- Any cases from the previous period which have been passive during the whole overlap period, but which nevertheless cannot be finalized at the end of the overlap period

To the terminated period (records section for remote storage) belong those cases which were finalized during the concerned records period.

It should be possible to use the system of overlap periods in Noark-4 for most period divisions, far more than in Noark-3 and Koark, cfr. sub-chapter 12.5. However, this presupposes a careful definition of records sections and the relationship between them (predecessor/successor). Through the definition of records sections, it is possible to use an overlap period even if the filing plan is modified, and even if organizational changes are made within the organization which the Noark base covers.

When changes are made which make it necessary to move the records to an organization that does not use the same Noark base, it will be necessary to use some kind of *sharp period division* where singling out/remote storage/transfer is carried out as soon as a period has terminated. However, even in such cases, a careful definition of records section is useful in order to provide for orderly conditions. It is also recommended that notes on records sections be used in order to document what has been done.

12.3.2 Remote storage of object-sorted records sections (object series)

In object-sorted records sections, it will often be appropriate to let the remote storage follow the objects, i.e., no periodization is carried out within the cases relating to one object; instead, the entire file for the object is stored simultaneously. This is because cases relating to certain objects may be of interest for a long time, typically for as long as the objects themselves are of interest to the organization. Examples of such material are personnel files relating to the employees of the organization, client files, student files, property files, etc. Cases relating to other object may, on the other hand, soon be of less interest due to a loss of interest in the object itself. This may happen when an employee leaves the organization, a client relationship is terminated, a student leaves, a property is sold, etc.

An obvious remote-storage principle for such material would be to *store the entire file for those objects which are no longer of interest*. However, it is not advisable to just store away the files as soon as employees leave, properties are sold, etc. The remote-storage records must follow the same sorting principle as the active records, and it is thus necessary to make sure that the remote-storage material is sorted according to this principle - alphabetically by person name, in ascending order of "gårds- og bruksnummer" (i.e., farm- and farm-unitnumber), etc. For practical purposes, the material must be divided into time intervals, i.e., sorted according to the relevant sorting principle within that time interval (period) and then packed in cases and stowed away. The same records periods should be used as for the topic-sorted records sections within the same records entity, since this makes it easier to keep track of things and provides for consistency in remote-storage records material.

In the Noark base, one records section is defined for each object series which is to follow this remote-storage principle, and for these records sections a case date and records status A ("active") are registered. Such records sections are, in principle, "eternal", i.e., they exist as long as the object series is used, and their status does not change.

For remote storage of such records sections, two alternative procedures may be used:

Option 1:

- At the end of a records period, or two years later when the overlap period for the topic-sorted records sections is terminated, a separate records section for remote storage is created from each object series for the terminated period. These records sections get records status B ("bortsatt", i.e., stored in a remote location), which means, among other thing, that it is blocked against normal registration. As successor to an individual records section having status B is registered the corresponding records section in the active records entity (which has status A).
- The object-sorted records sections of the active records entity are searched through, and objects which during the terminated period have been classified as having no current interest, are retrieved. All cases relating to these objects are then transferred, using a collective command, to the appropriate records section for remote storage, and an end date is registered for this records section (= last date in the terminated records period).
- In the physical records, the files for each object that is no longer of interest, are removed from the active records and stored in a remote location, in the same order that they had in the active records.

Option 2:

- Separate records sections for the remote storage of objects of no current interest from the individual object series of the period are created already at the start of a records period. These records sections get status U ("uaktuell", i.e., of no current interest) and are blocked against normal registration. As successor to each records section is registered the corresponding records section in the active records (with status A).
- In the physical records, separate "divisions" (cabinets, drawers, filing jackets, etc.) are reserved for remote storage of objects of no current interest from the individual series.
- As objects are deemed of no interest, all cases relating to the objects are moved, using a collective command, to the appropriate records section for remote storage. The object file in the physical records is moved to the reserved location for remote storage. These operations may be carried out periodically rather than individually, for instance by

moving all objects which have been judged as being of no current interest during the last year.

- At the end of the records period, the status of the concerned records sections changes from U to B, and a new end date is registered. New records sections having status U are created to continue the process, cfr. the first indent. The successor to a records section with status B is changed into a new records section with status U, and the successor to this is a records section in an active records entity (having status A).
- In the physical records, remote storage is simultaneously carried out for those object files which through the above procedure have been set aside for remote storage.

In electronic records, the division into records sections follows automatically from the registrations in the records management system. Remote storage of electronic records is part of the reorganization procedures for the Noark base, cfr. 12.3.4 below.

Not all the object-sorted records sections described below are likely to be suitable for remote storage according to the procedures described above. It may occasionally be appropriate to follow the same principles as for topic-sorted records sections, in which case the procedure in 12.3.1 is followed. In other cases, there are objects which will "always" be of interest. Even so it may be appropriate to follow the regular periodization that applies to topic-sorted records sections, but in such a way that for instance the latest two records periods are always kept in the active records.

12.3.3 Remote storage from records sections sorted according to board meetings

Records sections which are sorted according to board meetings, contain minutes, summons, case plans, etc. The documents are associated with individual board meetings, and because of this they are sorted chronologically according to the date of the meeting and board case number. The material is not registered. It constitutes a separate record series and is not linked to the structure of the case records in a recordkeeping sense (records management through case and registry entry). In terms of contents, however, there is an obvious connection, since the documents predominantly concern the handling of one or more cases from the case records (records cases).

Material which is sorted chronologically, is particularly suitable for regular period division and remote storage in accordance with this. The following procedure is recommended:

- The same records periods as for topic-sorted records are used.
- When a records period is terminated, the status for the concerned records section changes to B, and the records section is thus blocked against new registrations. The end date for the records section is registered (= last date within the records period).
- A new records section is created as successor to the terminated one. It gets status A, and new documents are linked to it.
- Documents in the physical records are stored in a remote location (cfr. rules and regulations for public records with regard to binding, etc.).

There is, of course, nothing wrong with postponing the remote storage until the end of the overlap period of the topic-sorted records sections. This will make it possible to carry out all remote storage in one operation.

12.3.4 Periodization and reorganization of the Noark base

It follows from the description above that the active Noark base may well include several records periods. This makes it easy to keep track of the most recent parts of the bulk of records, even those parts which are located in remote-storage records.

The active base should normally never be completely empty, unless fundamental changes are carried out in the records organization and system which necessitate this. The solutions presented above presuppose, as a minimum, that the base always contains the registrations of the last two years (the overlap period). However, it is generally recommended to always keep the last terminated records period in the base, and it may in many cases be appropriate to keep several - provided that the storage and handling capacity of the system is sufficient.

It is just as important that any reorganization of the Noark base (i.e., singling out of registrations and documents which are of no current interest) must include one or more *entire, terminated records periods*. The singled out records periods should normally be entered into separate historic databases. A historic database should always contain one or more *entire* records periods. It is also necessary to produce an export version of the singled-out material for transfer to archival repository.

The following procedure should be followed (see also rules and regulations for the periodization and transfer of records material from public administration):

- It is decided which parts of the base should be reorganized. This should cover all registrations and any electronic records associated with one or more entire records sections. All records sections must have records status B; they are in the following described as a finalized part of the Noark base.
- A report of the *records summary* type is produced (see paragraph 11.3.1) which covers all records sections included in the finalized part of the Noark base. The report is printed on paper and stored as part of the main documentation of the records entity, cfr. records plan.
- One or more transfer lists are produced for the finalized part of the Noark base. The transfer list(s) follow the specifications of paragraph 11.3.8 and are produced for each records section separately or as one list divided into records sections. See also the current regulations.
- Before reorganizations, the finalized part of the Noark base should be copied to "flat files" in the export format described in chapter 15. In addition, registrations from the same records period(s) that is/are later moved to other records sections, ought to be included, cfr. K12.16.
- One or more historic bases are established, covering the finalized part of the Noark base as well as any other registrations from the same period, cfr. the previous indent. Historic bases may be produced through import to a Noark system from an export format, or through direct copying from the active base.

- Files in the export format and historic bases must always be organized so that they cover one or more records periods, including registrations and any electronic records, as well as any other registrations from the same period, cfr. the above. The association with the corresponding physical records material in a remote-storage records entity must be documented well.
- When all the previous indents have been completed and its quality controlled, the finalized part of the Noark base may be deleted from the active base.

12.3.5 Transfer to archival repository

If periodization and remote storage is completed in accordance with the regulations and the procedures recommended above, the foundation will have be laid for a successful transfer in due time. This does, however, presuppose communication with the relevant repository institution in order to clarify the exact procedures of the transfer, including packaging and transportation, as well as choice of storage media for electronic material.

It is important to note that electronic material should normally be transferred at an earlier stage than hardcopy (paper) material. In connection with a reorganization of a Noark base, one should therefore plan the transfer as part of the procedure, including the communication with the relevant repository institution.

12.4 Changes from Noark-3 and Koark

Following is a brief summary of the major changes, all related to the *basic version* of Noark-4 (requirement type O). A complete technical specification of all exceptions is included in chapter 16.

- The definition of *records sections* and the relationship between these (predecessor/successor), see ch. 7 above, makes periodization more flexible in Noark-4 than in Noark-3 and Koark.
- The concept of *records period* in Noark-4 replaces the *registry period* of Noark-3 and Koark. Material from one records period comprises a physical unit in the physical records and a corresponding logical unit in the Noark base.
- Noark-3 and Koark presuppose that the division into periods is consistent throughout the entire base, and that remote storage is carried out simultaneously for all finalized cases. Noark-4 permits several different remote-storage principles, and these may be different for individual records sections. It is recommended that the records periods be the same for any individual *records entity*, but there is nothing to prevent separate records sections from deviating from this norm.
- In Noark-3 and Koark, the database should be reorganized simultaneously with the remote storage. In Noark-4, it is recommended that finalized records sections be kept in the base until the end of the next records period. When the database is reorganized, this operation should always include *entire* records sections.
- The principle of overlap periods is continued. Its use is recommended for records sections which use "regular periodization" as remote-storage principle, i.e., all finalized

cases within the period are stored simultaneously. Within such records sections, its use is recommended to a wider extent than what follows from Noark-3 and Koark, such as for the implementation of a new filing plan. A sharp division between periods is recommended only in special cases.

- Noark-4 describes the remote storage and periodization of records sections organized according to board meetings. This is not described in Noark.
- The export and transfer format in Noark-4 is completely new, specified in SGML. The format includes all parts of the Noark base, including the board-handling module and electronic records.
- Noark-4 presents electronic storage (in history database and/or export format) as the only solution for the preservation of reorganized data from a Noark base.