

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 filing¹. 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.

NOSIP² 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]³. 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 private character. The specifications assume that official e-mail receptions will be

¹ «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.

² NOSIP-2.0 - Norsk OSI profil. Statskonsult [the Directorate of Public Management], 1996.

³ «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.

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 <i>should not</i> be dispatched by e-mail. Note that this should not prevent an <i>informal</i> 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 <i>description of contents</i> 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 <i>Additional information</i> 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 <i>Dispatch status</i> 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 <i>Dispatch status</i> 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 <i>dispatch letter</i> 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, <i>Digital signatures</i> . 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 <i>Digital signatures</i> 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