ARBEIDS- OG
ADMINISTRASJONSDEPARTEMENTET

Summary in English: NOU 2001: 10

Without Pen and Ink

The use of digital signatures in electronic interaction with and within public administration

Selected chapters from the Norwegian Public Report 2001:10

Some chapters from Norwegian public report - 2001:10

Without pen and inc

The use of digital signature in electronic interaction with and inside public administration

2 Main conclusions of the Committee

2.1 Introduction

Developments within technology and society place great demands on the abilities of the Government administration to readjust. The Government must be able to deliver rapid, cost-effective services which are adapted to individual needs [21]. Renewal of the public sector is currently high on the political agenda. Important actions designed to renew the public sector include an emphasis on "24/7 administration" as a key tool. The aim of 24/7 administration is to supply public services in a cost-effective manner and on the users' terms, irrespective of time and place. Using the Internet as a communications channel is a fundamental element in realizing (implementing) administrative services of this type. In order to achieve 24/7 administration targets, the Government should establish suitable solutions for electronic case processing, the provision of electronic services and electronic administrative procedures, such as financial administration and procurement. Solutions ought to be integrated throughout the value chain, i.e. internal systems and external service systems, and must be effective across all sectors and administrative levels in order to produce benefits.

To support such solutions, a secure, efficient and reliable infrastructure is needed for the exchange of electronic information, which can ensure that electronic communication acquires the same legal validity as paper-based communication. The Internet is "the electronic highway" where information can be exchanged between different parties in different ways. The Government administration can interact electronically with individuals, companies can interact with the administration services and the Government can make its internal communication more efficient.

The Internet is basically not a secure network. Communicating electronically without knowing whom you are talking to, and without knowing if what you send is what reaches its destination, or if someone has read it en route, is not a good, safe solution for the communications needs of Government administration. The growth of secure, standardised solutions for authentication of the communicating parties and protection of the electronic information which is exchanged – digital signatures – may prove to be a sound, efficient solution to the problem.

Digital signatures and the accompanying infrastructure (PKI=Public Key Infrastructure) provide a way of knowing who the sender of an electronic message is (authentication), the ability to secure communications so that all attempts at making changes are discovered and stopped (integrity), opportunities for scrambling the contents (encryption) so that they are illegible to anyone else except the recipient (confidentiality) and a means of linking the contents to the sender so that he/she cannot deny having sent it (non-repudiation).

The great advantage of a Public Key infrastructure with digital signatures is that it can offer a coordinated security solution for electronic access to Government services, electronic reporting and other exchanges of information with and within the Government. Coordinated security solutions may be able to reduce the costs incurred by the Government administration when establishing and developing such services, and they may make using the public administration services easier.

Alternative solutions to digital signatures are available in certain areas (especially for authentication). However, there are very few, if any, standardised solutions which can support electronic signatures for non-repudiation. For applications in public administration, which need to be well secured against repudiation of transactions, digital signatures are a prerequisite for offering such services electronically.

It is not necessary to understand the “nuts and bolts” of a new technology to benefit from it, but a user must master the applications. Things that look simple to the user are often extremely complex and advanced “behind the scenes”. The introduction and use of digital signatures and accompanying infrastructure involve a number of technological, legal, organisational and administrative challenges. This is a complicated field for public administration to relate to. There is therefore a need for a policy on this area, covering norms for use, basic principles for setting up, introducing and maintaining the infrastructure, and strategies on how public administration should ensure that it works in accordance with assumptions.

This report proposes basic elements for such a policy.

2.2 Recommendations regarding individual mandate items

2.2.1 Types of certificate and identification

In order to use digital signatures on a large scale, a digital certificate is required. Such certificates serve as electronic proof of identity of the owner and guarantee that the digital signature really belongs to him/her.

The Committee has discussed who will require such certificates, what information the certificates should contain and how the information should be interpreted, and in particular how to identify natural and legal persons in a reliable manner in such a certificate.

The Committee wishes to point out that the issues under discussion here are fundamentally an international concern, and its recommendations must be seen from this perspective. Comprehensive international and European standardisation work in this field is currently being carried out, and the adoption of the EU Directive relating to Electronic Signatures lays down clear conditions in respect of the choices which can be made.

The Committee has attempted to use this as a basis for its recommendations, at least where the situation in the international arena has been clarified at the time.

The Committee has concluded that four types of certificate might be needed for communication with and within the Government administration:
- Civil servant certificates (certificates for public administration employees),
- Organisation certificates (server certificates or "role" certificates),
- Public access certificates (certificates for private citizens),

– Certified professional certificates (personal certificates for self-employed professionals, which link individuals to a specific profession/education and possible authorisation/approval from an official agency or organisation).

The Committee recommends that these certificates should contain information which can be coded and interpreted in accordance with profiles[1] based on international and European standards. Profiles relating to the four defined types of certificate are attached to this report.

The Committee recommends that certificates for public administration employees should contain either an employee number or a unique personal code for unique identification, where this is necessary in order to distinguish between two employees in the enterprise.

The Committee recommends that certificates for natural persons (public certificates) should have identifiers which are allocated by a certification service provider, and which are unique for each person within the certification service provider's domain. Such identifiers (figures and/or letters) should not be the same as thepersonal ID (PID) number issued by the state. The provider must establish a link between the unique number and the date of birth. Those government agencies which are officially required to do so may obtain access to the certificate holder's PID-number via the certification service provider.

This should be eliminated in cases where an official agency has a valid reason for making direct use of the PID number in a certificate (e.g. the national insurance service).

The Committee sees no need for a person's full name as registered with the Norwegian Population Registry to appear in a certificate if the certification service provider has checked it before issuing the certificate concerned. The certificate will show the name normally used by the person in question. By checking entries in the Population Registry, the certification service provider must verify that the correct person receives the certificate.

The Committee recommends that organisation certificates should contain the organisation number registered with the Central Coordinating Register for Legal Entities (*Enhetsregister*) in Brønnøysund as a unique identifier. For professional certificates, the Committee recommends that a number from the relevant register of personnel in the professional group in question should be used as unique identification. An example of such a number might be a health personnel number. The use of professional certificates is being discussed in the health sector.

The content of certificates may vary depending on the type of certificate, and from one certification service provider to another. Whenever a certificate is to be processed automatically, there should be clear rules stating how the contents of each relevant information element should be interpreted and processed. This will create challenges

[1] A profile is a precise definition of a standard which has been adapted to suit a specific area of application.

when the Government receives certificates issued by unknown certification service providers, e.g. from abroad. As regards the handling of foreign certificates, the Committee would point out that discussion and organisation of this must be included as one of the tasks for the coordination function which is discussed in item 2.2.3.

The Committee's assessments relating to this mandate point are found in Chapter 7.

2.2.2 Security levels

In order to be able to sign digitally, the certificate holder is issued with a pair of keys (cryptographic codes), consisting of one private and one public key. The public key lies in the digital certificate, which is available to everyone. The private key is secret and should be kept in a safe place.

Each provider of digital certificates and keys must document that he/she satisfies the security requirements relating to the issue, handling and maintenance of certificates and keys. Such documentation is called certificate policy and the certificate practice statement, respectively. Certificate policy provides a picture of the security level of a certificate.

The Committee has discussed the need for different security levels for certificates, which the public administration can use internally or which users can use in their dealings with the administration. The Committee proposes three basic security levels for digital signatures/PKI solutions, which can be used by the administration.

Level 3 involves storing certificates and their accompanying private keys on smart cards, and the calculations being carried out on the card. Level 2 distinguishes itself in terms of security from level 3 because the keys and certificates do not need to be stored on a smart card, but can be stored, e.g. encrypted, on a PC or a special diskette.

The Committee recommends that secure and reliable encryption algorithms are used for both levels, and that certificate holders must attend personally at least once in order to undergo definite identification in connection with the issue of a certificate for digital signatures. There should also be secure procedures for handing over keys and certificates to owners.

The Committee recommends that three separate pairs of keys should be generated for each certificate holder, with each pair having its own use. The three pairs of keys should be used respectively for signature, authentication and encryption.

The Committee believes that it may be necessary during the transitional phase to use just two pairs of keys because existing solutions on the market only support three separate pairs of keys to a limited extent. When using these, the Committee recommends that functions associated with these two keys should be divided so that the encryption function has its own key. The Committee believes that administrative limitations can be imposed on the use of a combined key for signature and authentication functions where necessary. Such limitations may mean that a key is only to be used for signing, for example, even if it is also designated for authentication.

The Committee also recommends that access to private keys should be secured by a PIN code or an adequately secured password.

Level 1 covers certificates which do not correspond to levels 3 and 2, i.e. certificates with a lower degree of security. PIN codes and passwords used directly for electronic interaction/access to systems will also be covered by this level.

The Committee does not wish to make any security recommendations for this level.

The Committee recommends that a joint certificate policy should be drawn up relating to the issue of certificates at level 3, and that a similar joint policy should be drawn up for level 2. These policies should be based on the Public Administration Network Cooperation's certificate policy no. 1 [2] and the ETSI European standard, Policy requirements for certification authorities issuing qualified certificates [3]. The joint policies which are to be drawn up should also be adapted to take into account the certificate types and profiles recommended by the Committee.

The Public Administration Network Cooperation's certificate policy FSP-1 should be adapted to suit the unique identifiers recommended by the Committee, coordinated with the ETSI standard and the new recommended certificate profiles. The Committee does not recommend compulsory use of joint certificate policies by the public administration.

The Committee's recommendations on this point are based on the current availability of the relevant technology and the extent to which it has been standardised. It will be possible to amend the Committee's recommendations if developments alter the fundamental conditions in this respect.

The Committee's recommendations relating to this mandate item may form a basis for the public enterprises' choice of security level for their electronic applications. A choice should always be based on individual assessment of each application. The Committee will not make recommendations as to which security levels will suit which applications, but it will provide guidance on usage, cf. recommendations relating to certificate issue models below.

The Committee's assessments relating to this mandate point are found in Chapter 8.

2.2.3 Certificate issue models and organisation of Government coordination requirements

The Committee has discussed different models for how PKI can be set up for use by the Government and their users in a cost-effective and suitable manner. Setting up the infrastructure means clarifying who is to issue certificates and with what security, who will ensure that certificates are issued to the correct owners (registration function), what sort of costs can be expected when using the infrastructure and who will cover them. Clarification is required in respect of both internal use by the public administration and users of public services and organisations with whom the public administration interacts.

The models discussed in this chapter concern the supply of certificates with level 3 or level 2 security. The Committee does not wish to comment on when level 1 certificates should be used. This is a choice which falls to each public agency wishing to make use of security solutions in respect of electronic communication. However, the Committee believes that when making such choices, much consideration needs to be paid to whether "heavy" security is necessary, or whether one can manage with lower level solutions.

The Committee recommends that the Government administration should be supplied with certificates for their employees by setting up a new, extended framework agreement relating to digital signatures and certificate services under the Public Administration Network Cooperation's procurement scheme. This agreement should also offer products and/or services making it possible for public bodies themselves to issue certificates to their own employees. Public administration certificates should primarily be level 3 security certificates, but the use of level 2 certificates cannot be excluded if requirements so dictate.

The Committee recommends that in order to supply certificates to individuals cooperative agreements should be entered into with at least two players on the market who issue, or will issue, certificates to individuals in connection with their own use of PKI. Such players may, for example, be banks.

The costs involved in using such public sector certificates should initially not be borne by individuals. Such certificates should have a minimum of level 2 security, progressing to level 3 when similar solutions are available on the market and are readily available to individuals.

The Committee recommends that more practical experience of the use of certificates in connection with electronic interaction between companies and the Government should be gained before joint actions can be proposed by the Government.

The Committee recommends that separate funds should be allocated for the use of digital signatures and PKI by the Government. Such funds should be allocated to projects where digital signatures are to be introduced in accordance with adopted joint schemes and recommended joint standards.

The Committee recommends that a permanent coordination function should be set up for the use of PKI for interaction with and within the Government. This function should be set up as a permanent committee with a secretariat and a separate operating budget. The committee should consist of key coordinating authorities and agencies at all levels of administration. The committee should be chaired by an IT coordinating ministry - either the AAD (the Norwegian Ministry of Labour and Government Administration) or the NHD (the Norwegian Ministry of Trade and Industry). This coordinating function should cooperate with the Norwegian Post and Telecommunications Authority and the Norwegian Data Inspectorate, which are the supervisory bodies with the statutory authority to deal with electronic signatures. The Committee believes that the mandate for the coordination committee and the work, location and funding of the secretariat should be the topic of discussion between the ministries involved and any subordinate bodies, as well as local government

representatives. The Committee believes that a discussion of this type should be commenced immediately.

The Committee recommends that, based on this coordinating function, a Forum for Digital Signatures should be set up, with representatives from the Government, industry and suppliers, in order to discuss joint PKI standards.

The Committee's assessments in respect of this mandate point are found in Chapter 9.

2.2.4 Interoperability

PKI is a complicated infrastructure from a technological, legal and organisational point of view. Many players participate in the infrastructure (cf. Chapter 3) with varying roles and responsibilities. This can create a number of challenges for users of the infrastructure.

The choice of strategy in respect of the establishment of PKI (cf. point 2.2.3) results in consequences which serve to further complicate the use of PKI. The desire to exploit market forces and the competition aspect entails demands being placed on market players to be able to work together so that their customers are not restricted in their freedom of choice in respect of who they can communicate with electronically.

As far as certificate users are concerned (i.e. people who receive a signature with a certificate on which they should be able to rely), the challenge lies in whether or not the certificate comes from a provider they know and trust, or whether it comes from a completely different provider about whom they know nothing at all. How can the security of such a certificate be assessed? Can one be sure that the signature is genuine? Could the provider have made a mistake when registering the certificate holder so that the latter appears under a false identity? Certificate users need answers to these questions if they are to make use of an open infrastructure where several players can provide certificates to various different target groups and where the users can select the provider they want
The challenges involved may also relate to the technology being used. Even though PKI standardisation has come a long way, there are still a number of ways in which it can be implemented which can create problems when the users of different signature and encryption software communicate and exchange digitally signed messages or documents.

The Committee has discussed the various aspects of the need for interoperability solutions in such an infrastructure. Its assessments are related to the need for different structures which can rectify trust problems associated with unknown certification service providers and the need for good cooperation between digital signature and encryption software from different suppliers.

The Committee recommends that the Government should contribute towards the establishment of trust structures in the market, such as cross-certification of providers, or a top node which certifies all providers within a given area. The Committee recommends that the Government should demand trust structures of this type for providers who have entered into agreements with the Government.

The Committee recommends that the Government and market players should unite in an initiative to set up a joint coordinated validation service which users both in the Government and the rest of society can make use of. The Committee recommends that the Government should play an active role in establishing such a service in the Norwegian market. If necessary, the Government should be able to provide part-funding for the initiation of such a service which should otherwise be based on commercial operational terms and conditions.

The Committee's recommendations in respect of this mandate point are found in Chapter 10.

2.2.5 Rules for the use of digital signatures by the Government

Based on a legal report, the Committee has discussed the need for regulating the use of digital signatures and the associated infrastructure by the Government and their users. This sort of use was considered in the context of other procedures that are necessary for electronic communication and document processing.

The purpose of these regulations is to describe the main principles involved in how electronic communication with the Government can and should take place, with the opportunity for adapting solutions to the needs of each individual administrative agency. Regulations are also proposed for in-house use of digital signatures and certificates by the Government.

The Committee is presenting a draft regulatory framework which provides specific instructions for electronic communication between the Government and individuals, and within the Government itself. These proposals include regulations relating to both authentication and signature, as well as the protection of confidentiality. The regulations are to be linked to the general provisions contained in the Public Administration Act relating to the processing of administrative cases.

The Committee recommends that the necessary regulations should be included in new provisions incorporated in the Public Administration Act and the Act relating to electronic signatures. Provisions can be drawn up on the basis of these proposals. The Committee believes that work on such provisions should be linked to the implementation of the eRegel Project (a survey of legislation preventing electronic communication and electronic administrative procedures) (cf. point 5.2.5) and the revision of the Public Administration Act (*forvaltningsloven)* which is taking place as a result of this project.

The Committee believes that internal administration matters relating to the requirements, approval and procurement of security services and products for the Government, as well as regulations relating to internal case processing, should be included in the same provisions, unless there are strong indications to the contrary.

The Committee believes that the legal effects of using systems chosen or approved by the Government, or certificates belonging to them, must be made apparent in the regulations appurtenant to the Act which authorises them, or in the Act itself.

The Committee believes that it should be possible to coordinate the regulations relating to protection instructions in respect of handling electronically-communicated classified documents with the regulatory framework proposed here.

The Committee's assessments in respect of this mandate point are found in Chapter 11.

2.2.6 Electronic identity cards

The users of public electronic services will want the security solutions employed to be simple to use, reliable and secure. In order to comply with such wishes, the public sector will need to coordinate the security, solutions e.g. by implementing digital signatures and the associated infrastructure. Electronic ID (identity) cards are a coordinated solution of this type which could provide the users of public electronic services with a "universal" key to administration on the Internet.

An electronic ID card is a smart card which contains an electronic identity – an EID. EIDs consist of three pairs of encryption keys and their accompanying public key certificates for use for digital signature, authentication and document encryption, respectively. A certain amount of information about the owner must be printed on the cards, but they do not necessarily need to function as an ordinary physical identity card. It should be possible to use such electronic ID cards for electronically signing and encrypting documents or for logging on to the Government's electronic services, at home, at a government office or other public place where it is possible to log on to Internet services with such a card.

The electronic ID cards in question are to be issued by a government agency that can assume responsibility for correct identification and verification of card owners, and which can guarantee secure delivery and withdrawal procedures, as well as a secure infrastructure for the use of such cards.

The Committee has looked at a similar solution which has been established in Finland. The Committee has observed that in order for such a solution to work, a great deal of coordination has to take place between the actual ID card solution and the development work undertaken by those government agencies that wish to make electronic interactive services available on the Internet. Much indicates that the Finnish authorities have experienced problems with such coordination, since the range of public services available where an electronic ID card can be used is limited at present.

The Committee has noticed that there is still not a wide range of PC equipment available on the market where smartcard readers have been integrated as standard features, and that the extent of such equipment in Norwegian households is almost non-existent. This situation may change when private players offering electronic services with card-based security features start to appeal to the population at large. The first test in this respect would appear to be *Norsk Tipping* (the Norwegian National Lottery) with its electronic pools card which is undergoing trials in 2001.

The Committee believes that the establishment of such an arrangement would require major investments and a major process before it could be implemented. The Committee believes that, based on market considerations, care needs to be taken when setting up public-sector services in an area where solutions exist on the market.

On the basis of these provisional assessments, the Committee does not recommend that the Government should start setting up their own public scheme for the issue of electronic ID cards now. The Committee believes that, on the basis of social and economic assessments, and in order to avoid duplicating the work involved, the Government should consider, on a continuous basis, using ID cards offered by commercial players on the market. This is also consistent with the strategy for supplying individuals with certificates as recommended in point 2.2.3, when such certificates are offered on smart cards.

The Committee recommends that the market situation should be monitored closely (both in Norway and abroad), and that experience should be acquired before engaging in any further analysis of the matter.

The Committee's assessments in respect of this mandate point are found in Chapter 12.

2.2.7 Financial and administrative consequences of the Committee's recommendations

The Committee's recommendations entail the establishment of a new, permanent coordination committee which should cover the public administration services in their entirety, including regional and local administration. In addition, the need for the committee to have a secretariat could lead to the establishment of a separate agency or the placement of a function within an existing agency.

The Committee's recommendations entail the establishment of a forum for the exchange of experiences between the various public administration services, trade and industry and suppliers of digital signature solutions. The Government should take the initiative, but otherwise participate on equal terms with the other parties involved.

The Committee's recommendations involve the establishment of a new framework agreement for the Government with solutions for digital signatures and PKI. Such a framework agreement should come into force within a reasonably short time following the expiry of the Public Administration Network Cooperation's current framework agreement (1 June 2001).

The Committee's recommendations entail negotiations taking place between the Government, represented by the coordination committee, and players on the market, with a view to setting up an agreement relating to the issue of certificates to individuals.

The cost of having a secretariat to deal with such a coordination function is estimated at approximately NOK 6.5 million per year (1-2 man-years, plus operating budget). The operating assets could be used for reports, preparing the basis of framework

agreements, developing common security requirements and evaluating solutions on the market. They could also be used to finance participation by the Government in the joint experience forum and for any contributions made towards establishing a joint coordinated traffic service.

Public agencies wishing to appoint members to the permanent coordination committee must fund such participation themselves. Estimated resources correspond to 2 months of work per year for each participant and 4 months of work for the chairman.

The activities of the joint experience forum are to be funded by the participants.

The Committee recommends that incentive funds should be allocated to stimulate the use of digital signatures by government agencies amounting to some NOK 9 million in 2002. It should be possible to allocate these funds to projects where digital signatures are used in order to support electronic services provided to individuals and to enterprises, both at central and local government level. The Committee believes that one of the criteria for the allocation of funds should be that the projects concerned make use of the joint solutions that could be set up. The Committee refers to a similar investment which took place in Denmark in 1998-1999, where the evaluation report presented during the autumn of 2000 concluded that the investment had benefited the Danish Government.

The Committee's assessments in respect of this mandate point are found in Chapter 13.

2.3 Proposed future study

The Committee believes that the handling of foreign certificates needs to be looked into more closely, especially in the light of the implementation of EU Directive 1999/93/EC in the EEA area and solutions in non-EEA countries.

The Committee also believes that a study should be undertaken of how the possible issue of professional certificates could be resolved. This should be done in cooperation with the authorities and organisations which are responsible for keeping the relevant registers of professions/qualifications which award rights.

In connection with the Committee's recommendation that the Government should contribute to a joint coordinated traffic service for certificates on the Norwegian market, the Government administration should define their requirements for such a coordinated traffic service. The Government should also review which common requirements should be placed on the verification information which emerges when processing certificates.

Another issue the Committee believes should be investigated in more detail is whether or not the Public Administration Act should be opened up for fully-automatic decision-making processes, and which requirements this would place on systems, documentation, etc., as well as the sort of vulnerability this would create.

The Committee believes that it is natural that the above-mentioned studies should be initiated and implemented under the auspices of the proposed coordination committee.

Apart from these studies, clarification will be needed when reviewing the processing of digitally-signed documents on a number of issues relating to the specific introduction of digital signatures and PKI in individual sectors, enterprises, and also in certain areas of application, including issues relating to internal procedures for archiving and the receipt of e-mail. The Committee sees a need for the development of procedures when using digital signatures for electronic case processing, the electronic management of finances, electronic public-sector procurement, etc. This work should be undertaken under the auspices of the relevant ministries and departments involved. The Committee believes that the proposed coordination committee ought to be included in this work as well.

11 Proposals for the regulation of the use of digital signatures and document encryption in the public administration.

11.1 Background

This chapter contains a discussion and outline for a possible *regulatory framework* relating to how digital signatures and encryption can be used with and within the public administration. Neither the new Act relating to electronic signatures nor the eRegel Project cover the needs and requirements for specific regulation for which proposals are presented here. Nor do other parts of the Committee's recommendations. However, this chapter contains proposals on how the public administration more concretely can make use of the recommended solutions for digital signatures and encryption.

The Committee believes that there is need for a common basis for the adoption of the proposed solutions. This will partly help individual enterprises, and partly serve to avoid different lines of action.

The Committee believes that the regulations which are proposed and summed up in this chapter should generally be viewed in connection with the rules on electronic case processing. As regards the protection of the obligation of confidentiality, one finds the protection instructions, cf. final paragraph of point 1.2, and the Committee holds that electronic processing of information classified in accordance with the protection instructions should be viewed in connection with the regulations proposed by the Committee in this chapter. Both the protection instructions and (hopefully) the draft rules will be subject to further work on the part of the administrators responsible for the regulatory framework, and the Committee believes that this will be a good opportunity to look at the development of these regulatory areas in context.

Point 11.2 deals with the question of rules relating to signature and authentication, and point 11.3 deals with the regulations relating to content encryption. Point 11.4 contains some overall views relating to the establishment of security services for the public administration. Point 11.5 discusses whether or not it is a good idea to have guidance (guidelines) or binding rules in the form of legislation or regulations. In point 11.6, the Committee provides an overall outline of its recommendations.

The eRegel Project ("Kartleggingsprosjektet" - the Mapping Project [47] points out that the extent to which one can/should open up for electronic communication in a statutory provision must be assessed on the basis of the actual provisions concerned, as well as other relevant provisions.

Case officers who shall make use of digital signatures and encryption in their work may need rules for when such techniques can be used, and how they should be used in different contexts [62]. Usage will vary from institution to institution and lies partly outside the Committee's mandate.

The Committee's recommendations are intended as a basis for future work and discussion on how to produce the necessary regulations. Its recommendations are not, and nor are they meant to be, fully processed draft proposals for legislation. Nor is it the Committee's intention to exclude other solutions than those outlined. Some of the proposals have been purposely worded rather bluntly in the hope of stimulating discussion.

11.1.1 Relevant issues

The Committee's recommendations pave the way for using several security levels and different models for the implementation of certificate services, etc. They allow individual public administration agencies to choose other security services than digital signatures. If a decision is made to offer public certificates, it would be natural for the public administration to build its solutions around these. Since no such decisions have so far been made, the proposed rules must attempt to embrace other solutions as well.

The use of digital signatures and encryption touches on general case processing. In its recommendations, the Committee has therefore attempted to deal with the borderline areas which touch on regulatory frameworks affected by the use of digital signatures and encryption, and to make proposals for developing these. This applies, for example, to general rules relating to electronic case processing and filing.

The internal organisation of ministries and departments in respect of who possesses the competence to sign or make statements in various different contexts, who signs what, is a matter which in any case in principle is independent of the use of modern communications technology. On the other hand an increasing degree of automation and "self-service" in the public administration, as well as changes in the flow of work with the introduction of electronic case processing, will serve to create new opportunities and challenges. The Committee has attempted to take this into consideration.

The core rules relating to the use of digital signatures and encryption will consist of provisions aimed at users – both internally in the public administration and at individuals communicating with the public administration.

A systematic distinction may be effected between 1) rules for the use of digital signatures and 2) reules for encryption. The need for respectively signature and encryption is triggered by different provisions, and the follow-up also follow different lines.

For example, questions relating to the choice of method for "signing" a complaint about an administrative decision, and the subsequent assessment of whether or not the complaint should be processed or rejected, will come under the Public Administration Act's rules on complaints. At the same time, such communications may be subject to

confidentiality in accordance with the Public Administration Act. The same considerations do not apply in these two cases. Nor is there any connection between sanctions in the event of a breach being committed.

Such messages may also be subject to requirements relating to the security of personal information in accordance with the Personal Data Act. These provisions probably cover both sets of regulations mentioned, since it is necessary in the circumstances to secure data quality, integrity, confidentiality and accessibility.

There may also be need for coordination with the rules on the processing of documents/information that have been classified in accordance with the protection instructions. The Committee's work is limited to the civilian area outside the scope of the Security Act[2]. It is so far unclear to us which requirements will be made in respect of the electronic processing of documents classified in accordance with the protection instructions after the Data Security Directive ("datasikkerhetsdirektivet") has been abolished. However, consideration should be paid to whether it is possible to coordinate the requirements relating to the classification as "Confidential" in the protection instructions with requirements which follow from, for example, confidentiality obligations and the safeguarding of sensitive personal information.

We could envisage that general requirements will be introduced relating to the use of security services for more closely specified applications. For example, it is possible that the requirements for the use of signature technology may be linked to the relevant message's "legal status," e.g. whether the message will constitute a case document in terms of the Archives Act, eventually combined with the question of whether it gives rise to rights or duties for any of the parties involved, or whether the message will be subject to requirements in accordance with financial regulations. It is possible that messages which are *neither* case documents *nor* relevant as documentation in accordance with the financial regulation, should be entirely exempt from the guidelines relating to the use of authentication services or signature technology. Such messages may require integrity and/or authentication services.

Even though a message is exempt from requirements for authentication services and signature technology, it may nevertheless be subject to requirements for content encryption. For example, the message could be linked to committee work and contain information which is not public, but is not nevertheless a case document for the agency in question.

Because the needs for security services may vary between different public administration agencies and individual applications, the recommendations allow for a certain degree of freedom for the agencies concerned to themselves choose the solution they find most satisfactory and suitable, possibly within the framework of alternatives drawn up by a coordinating agency for the public administration.

Official procurement of tools/systems/solutions in respect of digital signatures and encryption is not covered by the guidelines and constitutes internal processes which do not need to be incorporated into guidelines directed at others. This gives greater

[2] Act relating to preventative security services of 20 March 1998, no. 10, with appurtenant regulations (not in force).

flexibility in regard to exploiting the opportunities available in the future development of security services on the market. On the other hand, guidelines for use must be incorporated in a regulatory framework which is also binding for others than the public administration itself.

11.1.2 Relationship to the Act relating to electronic signatures

The Act relating to electronic signatures [52] implements Directive 1999/93/EC and deals primarily with the question of activities of certification service providers and functional requirements relating to, and the legal effects of, so-called "qualified electronic signatures". The Act touches, to a very limited extent, the rules on use of electronic signatures, and it does not deal with the question of content encryption.

The Act provides little guidance if the public administration were to choose to base its solutions on something other than qualified certificates and so-called secure-signature-creation devices,. The Committee assumes that other solutions can be chosen in addition, and that it is therefore necessary to touch on certain questions which are also dealt with in the Act.

11.1.3 Relationship with the eRegel Project

The question of which of the different legislative form and procedural requirements can be fulfilled by using electronic communication and electronic signature, and any eventual changes in the requirements of the law is not a major concern for the Committee. These questions are being assessed by the ministries concerned as part of the eRegel Project. As part of this process, one aspect that needs to be addressed is the purpose behind individual form and procedural requirements. This report assumes that the necessary adjustments are being implemented.

On the other hand, the regulatory framework recommended to be developed on the basis of the proposals contained in this chapter will constitute a framework on which regulatory administrators can rely when considering whether to allow electronic communication, and when choosing solutions for how this might be carried out in specific areas.

Even though the legislation contains no form or procedural requirements which prevent electronic communication or make demands for the use of security services, there may, for example, be evidentiary circumstances or risk assessments which make it appropriate or necessary to make use of such services.

11.1.4 Language and terms in this chapter

The draft regulatory framework has not been subjected to any separate treatment relating to linguistics or technical rules. This has not been necessary for this purpose, and given the time and resources available, it would not have been possible either.

No unambiguous definitions have been drawn up, but a description of how some key terms are used in this chapter may be appropriate, since the chapter ends with an

outline of what the Committee believes ought to become a regulatory framework. Terms such as "message," "enquiry," "document," and "material" can be synonymous with each other, depending on the context. No consistent distinctions are made between "data" and "information." On the other hand, the term "information" is used as a neutral term which can cover both meanings of the word. Terms such as "public administration agency," "agency," "department" and "enterprise" may be used instead of each other without any real differences being intended. Terms such as "citizen," "the individual," "individuals" and the like are used to refer to people who communicate with the public administration in another capacity than that of an employee of the public administration.

The terms "electronic signature" and "digital signature" are used as they are currently used in this field.[3] The terms "signature keys" and "encryption keys" are used about data which is used in connection with digital signatures[4] and content encryption respectively.

However, there is a problem, because some of the regulations are supposed to apply to both digital signatures and their accompanying certificates and to other signature and authentication techniques, e.g. PIN codes and passwords, if the public administration agency concerned uses such solutions. In some cases it will be possible to jointly process PIN codes/passwords ("authentication data") and public keys "signature-verification data") e.g. by requirements relating to the authentication of messages or the verification of signatures. In other cases it is authentication data and signature keys/private keys ("signature-creation data") which are jointly processed, e.g. by requirements relating to the safekeeping and use of keys or PIN codes/passwords.

Signature-verification data can, depending on the circumstances, be referred to as "certificates" in the sense that the certificate represents the link between signature-verification data and the distinguishing symbol or the characteristics of the certificate holder which one is trying to confirm. Making rough simplifications and also talking about the use of codes and certificates in situations when one is really thinking about the use of a signature key can be tempting at times. However, this would serve to perpetuate some of the misunderstandings which exist in respect of what certificates are, and how they are used. Until further notice, the Committee is unable to see any way round using the longwinded terms such as authentication data, signature-creation data and signature-verification data in connection with the outline of the regulatory framework being proposed here.

---

[3] Here "digital signature" means the application of systems for public key encryption and certificates issued and administered within a public key infrastructure (PKI). "Public key" refers to the fact that the key is available to the public – not that it necessarily has any connection with the public authorities. "Electronic signature" means the further application of authentication techniques as defined in the Act relating to electronic signatures, cf. Section 3, no. 1.

[4] No distinctions are made here between private keys used for signature (non-repudiation in technical terms) and authentication (called "digital signature" in a certification context when "signature" is undertaken using a hash value for authentication purposes without intending to "bind oneself" to the contents of the data basis from which the hash value is derived). If different keys are used for these purposes, and this is to be preferred, the key certificates will show which functions individual keys have.

11.2 Signing and authentication

11.2.1 The need for coordination and the desire for flexibility

There would appear to be an inherent contrast between the need for coordination and the desire for flexibility in respect of methods of communication and security services for different types of communications.

On the one hand, individual public administration agencies and individual citizens may want to be able to themselves choose what they consider to be a suitable and satisfactory security service.

On the other hand, it is obviously a challenge for the public administration to administer lots of different solutions internally, and for individuals to have to relate to all of these.

One possibility is to let the public administration agencies choose different solutions, e.g. digital signatures and PenOp[5], but with a requirement for cooperation between all the different public administation agencies. It is probably difficult to achieve any form of effective cooperation between so many different types of solutions within the various agencies. On the other hand, it might be possible to achieve such an effect if the agencies concerned employ different ways of implementing digital signatures.

Another possibility is to reduce the number of security levels to a minimum and allow as much communication as possible with the public administration to take place without security solutions or based on solutions which are supplied with a standard net reader (e.g. SSL). In return one could demand a higher security level when the requirement for safety becomes important. We must not lose sight of the fact that much of the communication which takes place between individuals and the public administration is trivial – it makes no major demands on security, and there is no point in regulating it. This should also be available through electronic aids to parties who do not wish to participate in "full electronic case processing and communication." In other words, no demands should be made other than those which can be met by any PC linked up to the Internet with "state-of-the-art" software – unless setting more requirements is absolutely necessary.

If requirements are first made over and above those which can be met by the standard configuration of an "average computer," it is less critical to raise demands to a level which can satisfy a greater number of needs . The use of digital signatures based on so-called qualified certificates is obviously one possible level.

In Sweden, the State Treasury has recommended three security levels, see point 6.1. The lowest level is not expected to have any coordinated solutions between public administration agencies, and a "medium-high" level is assumed adequate for most applications[6].

---

[5] Encryption of a visual signature on a document. http://www.penop.com.

[6] Cf. Swedish State Treasury, *Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster* (Electronic signatures and electronic identification of official e-services), 25 August 2000.

11.2.2 Relationship with electronic case processing

The use of digital signatures, encryption and other electronic security services is closely related to electronic case processing in general.

Regulations and procedures for receiving and handling enquiries, for keeping case logs and filing, for the internal flow of cases and for notifying people about the outcome of their cases, will be relevant to determine which security measures are useful and necessary. For example, routines designed to ensure that encryption keys are not lost, such that data becomes inaccessible, would be different if all decryption takes place at a central mail reception facility or archive than if it is carried out by individual case officers. The protection of data internally in a department's own system can be carried out using other means than those used in respect of the outside world because the participants are known, and the public administration agency defines its own "rules" for access to and the use of their system.

The new draft guidelines relating to electronic mail in the public administration can be a starting point for assessing security services used in connection with certain aspects of electronic case processing.

However, electronic mail is not the only form of electronic communication that the public administration can be expected to use. On the contrary, it appears as though much case processing in the long term will be carried out using websites or similar solutions. In many cases, it will be in the form of fully or partially automated services. This provides other and better opportunities for controlling the flow of information between individuals and the public administration. public administration can control, to a large extent, which information individuals have access to in advance, where messages will appear in the reception apparatus, which message formats are used, which checks are required, etc. This allows for completely different possibilities to continuously check whether necessary information has been supplied and to provide users with immediate feedback. Public administration agencies have less control over these matters when using ordinary e-mail systems.

Solutions which are controlled by public administration agencies can also pave the way for the use of security services in a different way to e-mail solutions. In particular, solutions based on authentication using different types of PIN codes or passwords can be set up in public administration agencies' information systems without need for changes in the user's local net browser. It is also possible to set up links to guidelines and relevant catalogues, etc., in a manner which makes it easier for the user rather than using traditional e-mail.

The predictability which lies in such a structure will probably provide a stable framework for the use of digital signatures, etc. This does not exclude the use of e-mail when public administration agencies find that they are appropriate.

11.2.3 Routines and requirement for electronic communication with the public administration

The discussion of the following points must be seen in relation to the general provisions contained in the Public Administration Act relating to the exchange of information between individuals and the public administration. The Committee's recommendations, see point 11.6, are not meant to interfere with the Public Administration Act's regulation of the traditional flow of information, but rather to serve as a supplement which regulates the special circumstances which are applicable when using electronic communication.

11.2.3.1 Addressees in respect of enquiries sent to the public administration

It will probably be an advantage for a public administration agency if all incoming enquiries relating to that agency and its activities, are "channelled via" pre-defined channels responsible for the registration/logging and onward processing of these sorts of enquiries to the correct place within the organisation. Any (initial) verification of signatures or checks with other authentication mechanisms and security solutions which need to be used, could be carried out at this point. Some of the functions could be implemented automatically by the information system carrying out the processing work. This applies, to a lesser degree, to electronic mail.

It should therefore be possible for public administration agencies to specify, with binding effect, which addresses or tools/systems should be used for enquiries sent electronically to public administration agencies. In order to implement this, public administration agencies should also be able to return/reject an enquiry which fails to comply with the instructions, together with information about the correct routines to be followed.

At the same time public administration agencies should be able to address messages directly to case officers if the internal routines of the agency in question are equipped to do so. However, the fact that individual case officers have an e-mail address should not be sufficient.

Direct addressing presumes other internal routines, e.g. sharing of cases, logging of information and filing. The agency in question should accommodate this before allowing direct addressing for case processing. One could also consider that directly addressed incoming mail should either go directly to the mail reception facility or "deliver a copy" to the mail reception facility on its way from the mail server to the addressee. However, this would result in private mail also being delivered to the mail reception facility. If the message concerns the activities of the public administration agency involved, but has been addressed to the wrong person, this would cause the mail reception facility or case officer unnecessary extra work because the directly mailed message would have to be "recalled" and at the same time send it to the correct case officer.

There are also other disadvantages with direct addressing, e.g. follow-up when the person in question is absent, has stopped working there, etc. Wrong addresses may, for several reasons, result in things taking longer or resulting in other unfortunate

consequences for the sender, e.g. because the case officer may know less than the mail reception facility about handling misdirected messages and what information the sender is entitled to and needs. Direct addressing should therefore be reserved for those cases or types of case processing where there is either a special need for it or where it is at least clear that there are no special disadvantages involved.

To avoid uncertainty, the rule should probably be that if a public administration agency wishes to allow direct addressing, then this should be expressly specified. For example, it can be done by providing guidance on the agency's website or by a pointer on messages sent by the agency in question. This would serve to enhance predictability for users when introducing electronic communication and case processing.

Before allowing direct addressing to case officers, arrangements must be made for securing the confidentiality of messages. This presumes that one either allows encryption using the case officer's public encryption key, or that arrangements are made for a two-phase process where the message is sent encrypted to the agency's mail reception facility, etc., and forwarded directly from this facility using the agency's internal security routines. The choice of a solution may depend *i.a.* on the kind of information to be transmitted.

There may be special requirements for direct communication between employees working for public administration agencies, i.e. that the exchange of information between employees working for the same or different agencies is not initially channelled via the archives or mail reception facility, as happens, for example, when using the telephone or fax. This may be due to considerations of efficiency or the need to be able to communicate in writing when the mail reception facility is not manned. In such cases it is also presumed that internal routines have been observed, e.g. in respect of requirements relating to logging of records. If provisional processing and forwarding from the mail reception facility occurs automatically when the mail reception facility is unmanned, the need for direct addressing ought to be limited, but can of course exist in certain cases. Nor do all the same objections which apply to "external" communications apply here. For example, direct communication between case officers will often be based on more secure knowledge about who is the right addressee than when dealing with, for example, messages from private individuals. In addition, some public administration agencies will be connected to networks which protect messages against access by outsiders without using encryption keys linked to the individual recipient.

Nevertheless, thought should be given to whether there really is cause to process messages differently, at least those which are considered "case documents" in the eyes of the Public Administration Act, depending on whether they come from citizens or from a different public administration agency. Individual public administration agencies should decide whether they want one solution for incoming messages, or whether they want to make arrangements for alternatives. As considerations might vary in different cases, it should perhaps be possible to allow direct addressing just from other public administration agencies.

- Electronic enquiries sent to a public administration agency should be directed to the address given by that agency for these types of enquiries.

- If a public administration agency has set up a system for enquiries, or certain types of enquiries, via its own website/home page, electronic enquiries should be made in the manner set up.
- Electronic enquiries sent directly to case officers that relate to messages concerning the public administration agency in question, should only take place if the agency has set up its system for this and has expressly permitted such direct message in general or in certain cases.[7]
- Public administration agencies can reject enquires that have a different form or that have been directed to a different address or in a different way than prescribed or set up. At the same time, the public administration agency in question shall provide information about the correct address, form or routine. This type of information may be supplied by referring to or sending out guidelines concerning the circumstances.
- Public administration agencies can decide that sending messages concerning the public administration agency in question directly to case officers may only take place when such messages are sent from another public administration agency.

11.2.3.2 Enquiries which activate the duty to provide guidance– form-free enquiries

Enquiries sent to the public administration are multifarious in nature. They may relate to the gathering of information without obligation or consist of enquiries that activate an obligation to provide guidance, enquiries that actuate case processing but that are not subject to special form requirements, the exchange of information which by law shall take place in certain forms, and the exchange of different types of sensitive information. Requirements and routines need to be adapted to these.

In point 11.2.1, the Committee recommends that the use of security solutions should not be demanded in contexts other than those where they are deemed necessary. However, it may be difficult to provide precise descriptions in advance about when there is a need for, for example, reasonably secure identification. In order to avoid security solutions being demanded "for safety's sake" it should be possible for public administration agencies to seek additional information or demand the use of security solutions in individual cases where necessary. It should also be possible to lay down general requirements for certain types of enquiries, e.g. requirements relating to the use of digital signatures and/or content encryption.

If a public administration agency makes such demands, it should at the same time offer or provide instructions about the security services which comply with the imposed demands. Individuals cannot be expected to find suitable services themselves. For example, instructions can be provided through links or by providing relevant contact information to certification service providers who have been approved by the public administration agency concerned, or by the agency itself organising and offering, if necessary with the aid of a third party, the use of, for

[7] This entails no restrictions on a public administration agency's freedom to open electronic communications directly to case officers, but it does require the agency in question to state at the outset whether the internal routines are satisfactory, cf. the discussion above. A clear indication of which communication channels are supported by the agency will also help improve predictability for the users when introducing electronic communication and case handling.

example, passwords and PIN codes for the authentication for using the agency's information services.

- Enquiries sent to the public administration that are not subject to special form requirements, and that do not actuate case processing, may be sent electronically without using security services.
- In certain cases, a public administration agency may request information to confirm the identity of the sender or authorisation if this is important for dealing with the message in question.

11.2.3.3 Applications and other enquiries that activate case processing

Permission to demand "confirmation of identity or authorisation" will probably be too weak in a number of cases. It should also be possible to demand the option of authentication, non-repudiation and, possibly, confidentiality. This can be carried out, for example, by demanding the use of special security services such as digital signatures and encryption.

- Enquiries that actuate case processing, but which are not subject to special requirements as to form, can take place without the use of security services.
- Public administrationagencies may, in certain cases, request information to confirm the sender's identity or authorisation if this is important for dealing with the enquiry. The public administration agency concerned can also demand that special security services should be used.
- Public administration agencies can stipulate that such demands should apply generally to more particularly defined types of communications.
- Public administration agencies shall offer, or provide instructions about, services which make it possible to comply with requirements for confirmation of identity or authorisation or other requirements stipulated by the public administration agency concerned.

11.2.3.4 Enquiries subject to requirements as to form

Enquiries subject to requirements as to form may require mechanisms in order to secure both data integrity and the possibility to ensure confirmation of the sender's identity or authorisation.

- For messages which are subject to special requirements of form, public administration agencies can provide instructions about which tools must be used so that communication can be carried out in electronic form, including requirements for methods of ensuring confirmation of the sender's identity or authorisation. A public administration agency can also demand that special security services be used.
- Public administration agencies shall offer, or provide instructions about, services enabling compliance with requirements relating to the confirmation of identity or authorisation or other requirements stipulated by the public administration agency concerned.

11.2.3.5 Enquiries which do not meet current requirements

Recommendations in this area are envisaged to comprise both cases where the necessary security services are not used and cases where relevant certificates, etc. have been revoked or the signature cannot be verified for some reason.

- Public administration agencies which receive enquiries electronically which do not meet the current requirements relating to such enquiries, shall notify the sender without undue delay, and advise which measures need to be implemented so that the enquiry can be processed[8].
- Such instructions can be provided by referring to the published rules of the public administration agency concerned relating to the handling of that type of enquiry in question.
- Public administration agencies shall record the time when such messages are sent, and to whom they are sent.
- A record should be kept if the fault is such that it is impossible to identify the sender, and it is not possible to send notification.
- The general rules relating to rejection and redress contained in the Public Administration Act shall apply in respect of the circumstances mentioned.

11.2.3.6 Information about decisions

To make electronic case processing as efficient as possible, it should also be possible to provide information about individualdecisions in electronic form. This must be carried out in such a way that the person(s) to whom the decision is directed does not end up in a situation where there is a greater risk of suffering legal loss, e.g. by failing to meet deadlines for lodging complaints, than under the current system of paper-based information.

This means first of all that one must be sure that the party concerned is aware that the information will be sent electronically, e.g. by obtaining the consent of the party concerned. Secondly, it is important to ensure that the decision in question is only made available to the right party. Thirdly, one should attempt to determine a clear cut-off point for when such information shall be deemed to have been provided and deadlines for lodging complaints start to apply.

Because we have no tradition or experience for providing information in this way, there is a greater need for a clear cut-off point than would probably be the case for paper-based information. This lack of tradition and experience means that it is necessary to maintain a back-up solution. This means that people who, in spite of having consented to being provided with information electronically, fail for some reason to gain access to a decision, should be sent this information in the traditional manner and after a certain period of time has elapsed.
Information about individual decisions can be carried out electronically if the party to whom the resolution relates/who is entitled to receive such information, has consented to such.

- Notification about decisions should be made available from an information system suitable for the purpose.

[8] This is intended to comprise both cases where necessary security services are not used, and cases where relevant certificates, etc. have been revoked or the signature cannot be verified for some reason or other.

- The party to whom the resolution relates shall receive information that the decision has been reached, and about where and how the party concerned can obtain information about its contents, as well as a deadline for the last date when this can take place.
- The contents of the decision shall be made available to the party when the party concerned confirms his/her connection with the case to the information system on which the decision has been placed (authentication).
- The information system records the time when the party concerned has acquired access to the decision, as well as data confirming the connection which the party concerned has to the case.
- Notification is considered to have occurred at the time the party concerned has acquired access to the decision.
- If the party concerned has not acquired access to the decision within 7 days from the date on which information about the decision was sent out or was made accessible, notification shall take place in accordance with the regulations that apply to the provision of information about individual decisions in the relevant area when consent has not been given for electronic communication.

11.2.3.7 Complaints

If case processing otherwise takes place electronically, or special arrangements have been made for such, complaints against decisions of public administration ought to be submitted electronically. The problems involved in respect of what is needed in order to fulfil the requirements of the Public Administration Act, which stipulates that a complaint should be signed, are not discussed here, cf. Section 32 (b) of the Public Administration Act.[9]

- Complaints relating to individual decisions can be sent electronically if a public administration agency has set up its system for such, or notification about the decision has taken place electronically.
- The public administration agency can request information that confirms the sender's identity or authorisation if this is necessary to handle a complaint. The public administration agency concerned can also request the use of special security services.
- The public administration agency shall offer, or provide instructions about, services that enable compliance with requirements relating to confirmation of identity or authorisation, or other requirements stipulated by the public administration agency in question.

The Public Administration Act contains rules about what is required to interrupt a time limit for lodging complaints. However, complaints submitted using "user-controlled" electronic communication, e.g. ordinary e-mail, are hardly likely to be dealt with under the special regulation relating to complaints submitted to postal or telegraphic stations. An assessment should be carried out as to whether special regulations should be developed in respect of interrupting time limits when submitting

[9] Refer if necessary to the Kartlegging Project about this. The purpose of the guidelines here is to provide instructions about routines which can/shall be used if the law otherwise allows electronic communication to take place. It is assumed that the necessary legislative amendments are being considered during the current phase of the Kartlegging Project/eRegel Project.

complaints electronically, e.g. when a complaint is submitted via a dedicated information service which has been set up by a public administration agency.

A solution based on a requirment for public administration agencies to always acknowledge receipt of complaints they have received, could also be considered. In such cases, the complainant cannot assume that his/her complaint has been received until he/she has received a receipt.

However, it is not correct to transfer the risk for transmission errors or delays to the complainant when a public administration agency has facilitated electronic enquiries in connection with complaints.

One possible solution could be to link interruption of time limits to the time the complainant initiated transmission of the electronic message to the public administration agency, but with an obligation to follow up by acknowledging receipt and re-sending the complaint if the acknowledgement of receipt is not received within, say, 24 hours. This would, however, place a further burden on the complainant in respect of follow-up after a complaint has been sent. It also allows for the opportunity to maintain that the deadline had not been missed by claiming that the complaint had been sent just before the deadline ran out, but did not arrive. With short deadlines for checking signatures and any new complaints, this is hardly likely to acquire great significance because a deadline under such regulations cannot exceed, for example, the 24-hour period mentioned. Nor is it possible today to try to object that a complaint has been sent but not received, with regards to complaints sent by post.

In the event of deadlines being exceeded, the general regulations relating to redress shall apply.

One alternative is that complaints should be always submitted via dedicated information services so that the transmission of a complaint and acknowledgement of its receipt occur "as a single operation." This should probably be the main rule, supplemented by provisions relating to the handling of complaints sent in a different way.

- If a complaint is submitted electronically, and the public administration agency concerned has set up its system for the receipt of complaints through the use of its information system, this procedure should be used.
- A public administration agency receiving complaints electronically should immediately send an acknowledgement of receipt of the complaint to the sender.
- Complainants are duty bound to check that they have received an acknowledgement of receipt for submitted complaints[10]. If such acknowledgement of receipt is not received within 24 hours, the complainant shall submit his/her complaint again, stating when it had been sent the first time.

[10] In a dedicated system, receipts will be sent immediately, so that no extra checks are necessary. The regulations relating to special checks will apply primarily to ordinary e-mail. The use of e-mail for submitting complaints should be limited.

11.2.3.8 Access to information and documents in electronic form

Access to electronic archives should be allowed. This would mean a substantial increase in the right of access as the threshold for individual access is lowered. First of all, it is assumed that it is easier to request access from one's own computer than by letter or by phone, provided that the archives to be examined are properly organised. Secondly, the person concerned does not have to wait for a letter from the agency in question or attend in person. Access via a screen can, in many cases, be gained immediately after a request has been submitted.[11]

If partial access is requested, and the document in question cannot be supplied under the Freedom of Information Act, it is important to ensure that the request has been made by the party himself/herself, and that the information is not made available to third parties when supplied. According to the Personal Data Act, requests for access can be submitted electronically, and the officer responsible for processing it can demand that the registered person (the person to whom the information relates and who has requested access) should identify himself/herself in a secure manner, e.g. by using a digital signature.[12]

As mentioned, access can be granted, for example, by direct authentication against an "access archive" (mirroring of documents for access purposes), or by the transmission of encrypted documents. This can be carried out by using a digital signature in connection with requests for access, and by sending documents in encrypted form or making them available on a dedicated information system in the same way as that which applies when providing information about decisions, cf. point 11.2.3.6.

- Requests for access to case documents or information can be submitted electronically to the public administration agency concerned.
- The public administration agency can, in some cases, request information to confirm the sender's identity or authorisation, if this is important for dealing with the enquiry. The public administration agency can also demand that special security services should be used.
- If a public administration agency has electronic archives, access can be provided in electronic form.
- Unless access can be requested in accordance with the Freedom of Information Act, online access will only be granted on the condition that satisfactory confirmation can be produced about the connection between the party concerned and the case, and that it can be guaranteed that the documents will only be made available to the party in question.

11.2.3.9 Hearing and comments for the hearing regarding regulations, etc.

---

[11] For further information about this, please refer to the Directorate of Public Management's report 1998:13 *Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering* (Legal approaches to problems relating to electronic case processing and document handling).

[12] Cf. Section 24 of the Personal Data Act, cf. Section 18. Section 24 states that the person responsible for processing a case can demand a written and signed request in order to ensure that it is the data subject and no one else who gains access to the information concerned. However, the comments to the individual provisions contained in Bill no. 92 (1998-1999) p. 122, states that requests can be submitted electronically provided that the data subject identifies himself/herself in a secure manner, e.g. by using a digital signature.

It will undoubtedly be expedient for public administration agencies if material to be circulated for comment can be accessed on a dedicated server instead of being distributed en masse in the form of postal letters.

However, it is essential that the people and bodies concerned are encouraged to familiarise themselves with the material relevant for the hearing. This can be done either by actively drawing the attention of the people concerned to the hearing, as is currently the function of the covering letter sent in connection with the hearing (hearing letter), or by otherwise making it generally known where the discussion material can be obtained at any one time, as is currently the procedure for certain types of public announcements.

Active notification could take place by using electronic mail. If this is to have the same effect as the hearing letterwhich is currently used, the recipient would have to have satisfactory routines for handling e-mail. This is particularly important in respect of discussions which directly affect the rights or duties of citizens.

Similar solutions to those which are used for providing information about individual decisions (cf. above) might be a good idea, i.e. where a traditional hearing letter is sent out if the consultative body fails to access the relevant material within a certain period of time. However, this could cause more problems than the case of provision of information because the discussions would not be based on direct advance contact between the public administration agency and the party concerned where consent to engage in electronic communication is obtained, but would be a "one-to-many" communication initiated by the public administration agency itself.

As far as discussions regarding the provisions contained in the Public Administration Act are concerned, it is the public administration agency itself that decides how notification should take place, cf. Section 37 of the Public Administration Act. However, the requirement for case information and the fact that those concerned shall be provided with a (real) opportunity to comment, involves certain minimum requirements being placed on the routines chosen by the public administration agency concerned.

If changes are to be made to current routines for hearings, e.g. relating to when individual notification should be made, a more thorough review of the consequences should first be carried out.

It should be possible to submit comments relating to a hearing's discussion documents in electronic form. The provisions contained in Section 37 of the Public Administration Act (relating to regulations) concerning written information are not really an obstacle in this respect. Since it may be important to know who has made comments, and in order to exclude the possibility of the wrong person making statements in another person's name, public administration agencies must be able to obtain the information necessary for verifying the identity of the person making the statement or authorisation, or demand security solutions. How great such a need is will depend on the topic under discussion.

- Hearing letters to addressees with their own/a central e-mail reception facility can be sent electronically. Instead of having the full set of the hearing letter and attached discussion documents, messages about where to find such a

document can be sent out with a request to access the document within a specified time. If the person concerned has failed to access to the discussion document by the specified deadline, the discussion document should be sent out in paper-based form, unless the public administration agency has decided otherwise in respect of the consultation in question.

- Comments may be submitted electronically. Such statements shall be submitted to the e-mail address specified by the public administration agency concerned in respect of the consultation in question, or in a different manner as instructed by the public administration agency.
- The public administration agency may request information to confirm the sender's identity or authorisation if such is important for dealing with the statement concerned. The public administration agency can also demand that special security services should be used.
- The public administration agency shall offer, or provide instructions about, services facilitating fulfilment of the requirements relating to confirmation of identity or authorisation or other requirements specified by public administration agencies.

11.2.4 Archives and long-term storage

According to section 5-2 of the Archive Regulations, archive material can be delivered to the State Archives (the National Archives of Norway and its regional divisions) after 25-30 years. Upon delivery, the recipient institution takes over responsibility for ensuring that the documents are accessible. According to section 5-8, "the Director General lays down specific requirements relating to material which is to be handed over to the National Archives." These requirements include the sorting, documentation, labelling, type and format.

Questions relating to archive formats for electronic messages equipped with electronic signatures are described to a certain extent in Noark-4 [57] (approved standards for electronic filing systems in accordance with the Archives Act and its appurtenant regulations). Considerations relating to the long-term storage of signed electronic messages also form the basis of some of the requirements contained in the current European standards for (extended) signature formats (ETSI ES 201 733). Proposals for standards without requirements for time stamping have also been drawn up (ETSI TS 101 733), and these were expected to be adopted during the course of 2000.

The standards mentioned above represent *possible alternatives* for the storage of signed documents, not binding requirements. It should therefore be considered whether any overall functional requirements should be made in respect of storage which *i.a.* the standards mentioned would fulfil.

The long-term storage of electronic documents[13] involves problems and challenges with which we are unfamiliar, or which are at least less urgent than the use of paper as a storage medium. In future, we will need to file such things as pictures, drawings and sound, along with other documents. Our definition of "document" as a limited amount

[13] Long-term storage in this context means storage beyond the period during which the case was being processed, not necessarily "long-term storage" from an archiving point of view.

of information could be challenged by electronic documents with hyperlinks to other electronic documents. Another challenge is that a document may look different when presented in a newer version of a word processing system than the one in which it was originally written. This could lead to changes occurring in the function of (central) archives, and the archiving function will probably become even more important than before. First of all, there may be a need for special equipment and skills in order to preserve the integrity of electronic messages over time. Secondly, it is possible that the archives of the public administration may also serveindividuals to a greater extent that is currently the case, cf. point 11.2.7.7.

There will probably be a number of cases or types of use of electronic communication where it will only be relevant to verify messages for relatively short periods of time after the actual transaction or exchange of information has taken place. If so, it is probably sufficient to demand availability of the verification data necessary for verifying the message as long as it is stored. This should be a minimum requirement for messages which, in accordance with the Archives Act or other legislation, should be filed, and may well emerge as the main rule.

However, there are several specific problems relating to the filing and storage of messages with digital signatures. First of all, certificates have a limited period of validity (often two to three years from the date of issue). After a certificate has expired, one can no longer base oneself on the certificate alone when verifying the signature. Secondly, the certificate may be revoked after the signature has been verified. If no measures have been adopted making it possible to date when the signature was added and when it was verified, one cannot simply build on the signature after the certificate has been revoked. In addition, security is weakened as time goes by. When filing, enough information should therefore be stored so that one can subsequently say that it was likely that the signature was satisfactorily verified at the relevant time.

This can occur, for example, by filing messages with different "time stamps" and other relevant information as defined in ETSI ES 201 733 Electronic Signature Formats (e.g. a complete chain of certificates and revocation data or references to such). For long-term storage, a so-called "archive time stamp" can be added.

Alternatively, the archive function can obtain necessary information and implement necessary verification. Messages can then be filed along with the archives' confirmation that correct verification took place at a certain time. In such cases, trust is not based on the possibility of repeating the verification process with a dependable result. On the contrary, the idea is that trust in the archive function and archive routines should establish the necessary confirmation that the link between a message and a certificate was acceptable on reception, or that satisfactory authentication was carried out in some other way, and that the archive has subsequently secured the message's integrity[14]. This approach may be relevant, for example, if a signed message is converted to a new format. The original signature can only be verified in relation to the format the message had when the signature was generated.

[14] ETSI TS 101 733 Electronic Signature Formats (v 1.2.2 (2000-10)), allows for such a model, c.f. the final sentence in the final paragraph of point 4.2.

- Messages that have been signed using a digital signature, and that are filed,[15] should be archived with a certificate confirming the signature and other information necessary for verifying the signature, including confirmation that the certificate had not been revoked when verification occurred.[16]
- For messages where the certificate's period of validity is shorter than the time it can take to confirm the contents of the message, and for messages which, when being archived or during the period of their storage, are to be converted to another format, the archive shall upon reception verify the signature and then provide suitable confirmation of the link between the message, the message's signature and relevant certificate with information about the time of confirmation. The archives shall ensure the integrity of messages and confirmation of the above mentioned matters during the period of storage.[17] The archives can decide that this approach should also be used for other messages (than those mentioned in the first sentence).
- If the archives fail to verify a signature, information to this effect should be stored, if possible with information about why the verification failed.[18]
- Messages or the results of automated data processing (e.g. from automated services with web interfaces) which have been confirmed using a different authentication technique than digital signatures, should be stored with information stating that correct authentication has taken place, and if possible which technique was used.[19]

11.2.5 Signing and verifying signatures – use of fully or partially automated systems

11.2.5.1 Signing messages that are processed manually

The signing of messages using digital signatures should probably follow the same rules which apply at any one time to similar messages sent on paper – at least as far as the contents are concerned.

---

[15] Emphasis has been placed here to show that it is not intended to impose a filing obligation on messages simply on the grounds that they have been signed using digital signatures.

[16] Confirmation of the fact that a certificate had not been revoked at the time when verification took place can occur in the form of time-stamped confirmation from the revocation list, and time-stamped confirmation from online certificate status protocols (OSCP), etc.

[17] As mentioned above, this can occur either by adding an "archive time stamp" as defined in, for example, ES 201 733 Electronic Signature Formats, or by the archive securing the message's integrity in some other way and documenting in a satisfactory manner the link between the message and the conditions which the certificate represents.

[18] Even though it is not possible to verify a signature during filing, it cannot be excluded that the message is relevant. First of all, it can be envisaged that a signature is not strictly required in the actual case in question, c.f. what is said in "Requirements relating to the control of certificates and revocation lists" under point 11.2.6.10 about the significance which a lack of verification has on the further processing of the message. Secondly, one could envisaged that the conditions which the message relates to are supported by other case information which thus contributes towards it being likely that the message's integrity is intact.

[19] This probably involves requirements relating to the filing of activity logs, etc. No requirements should be made in respect of the storage of authentication data as such. In code/password systems, this can involve a security risk. Possible alternative are the storage of authentication data in encrypted form or the storage of a one-off password. The latter places demands on the preservation of all used one-off passwords by the public administration agency concerned and the register showing when they were used, and is not really very practical.

However, a system is envisaged where digital signatures could be used for "sealing" messages where the "seal" identifies the issuing department (source authentication). Such a "seal" could have functions which are similar to the trust-building effect achieved through use by the public administration agencies' of printed letterheads and envelopes. Sealing using digital signatures also gives data integrity.

If an agency or enterprise can be identified by such a "seal," "digital stamp," or whatever it is called, it is probably not necessary for the recipient to identify the case officer from the signature. If it is important for the recipient of a message to know the identity of a case officer, this can appear on the actual message, as is currently the case. Very few of us are capable of identifying a sender on the basis of a signature. We find the necessary information in clear text elsewhere in the document.

Case officers' signatures, or those of their superiors, are an internal process which secures the contents of a message, and shows that the department concerned is responsible or answerable for such. The case processing system should ensure that messages are not passed on for "sealing" or dispatched until the requirements relating to internal case processing have been met. For example, it can ensure that the correct number of people or a person at the right level within the agency, have approved the message prior to dispatch, or that the relevant operations in respect of the type of case concerned have been registered as having been implemented, etc.

A "seal" that is added upon dispatch, or when the message is otherwise made available, should serve as confirmation of the fact that the internal processes have been adhered to – and thus the only thing the recipient needs to relate to.

The routines will involve channelling all department-related exchanges of information via one or more "communication centres." This will probably pave the way for efficient logging of information and the implementation of rights of access, etc.

The centralised job of sealing, etc., should be an automated function so that messages can be sent out or accessed on relevant information systems irrespective of whether or not the archives/mail reception facility are manned.

It should be possible for direct communication to be carried out between case officers working for different public administration agencies. This may be relevant *i.a.* in connection with internal administrative work on budgets, etc., which should both be kept confidential and which has to be communicated between case officers irrespective of whether or not the archives or the mail reception facility are manned.

11.2.5.2 Verification of signature on receipt

A centralised function might also be relevant when a department is a recipient. In other words, not just reception, and possibly decryption, but also verification of signatures and certificates should be carried out centrally – so that case officers can relate to the contents of a message as they appear to them.

This *could* facilitate the introduction of technology, training and information in departments, with a number of jobs being undertaken without individual case officers having to become involved.

The current ETSI standard for signature formats (ES 201 733) assumes that essential information and processing regulations could in time be represented and distributed in computer-readable form, as part of the signature in the form of reference to a signature policy, so that the recipient system can process the enquiry automatically.[20] It is envisaged that a signature policy will be linked primarily to specified types.

However, until further notice, a number of these issues will have to be resolved either locally by individual information systems, by cross certification and similar measures, or by being assessed by individual case officers. One should, as far as possible, avoid basing oneself on manual processing by individual case officers in respect of electronic signatures. Measures relating to the verification of signatures should be carried out either automatically or centrally at the agency, with the possible exception of assessing links between certificate owners and the relevant cases, which according to the circumstances could assume specific knowledge about the case or party in question. Individual case officers cannot, and should not, be expected or required to assess, for example, whether a given certificate policy or signature policy is suitable for this purpose.[21]

11.2.5.3 Enquiries which are processed automatically

In a number of cases, enquiries directed to the public administraiton will be processed automatically. This covers a broad range of matters, from making information, application forms and the like available in order to process standardised messages to automated decision-making processes.

In such cases, certificates related to persons in the recipient system will be without any real significance. There is no point in equipping an information system with certificates which point towards a person who has the necessary authorisation to implement the relevant transaction when the processing in its entirety is carried out by the information system.

The suitable thing would be for the system to "sign" directly on behalf of the department for the transactions which the system is "authorised" to process. In other words, when the public administration agency concerned is set up so that the system processing is decisive for the results, and the results are sent in electronic form directly to the person concerned, it should be evident that the message has been delivered by the agency as such, and the recipient should be able to adapt to this. One should not give the fictitious impression that someone with authority is behind the decision.

Routines need to be available in respect of the quality assurance and approval of such systems. Such routines must *i.a*. ensure that the relevant regulatory framework is

---

[20] Cf. for example ETSI ES 201 733 *Electronic Signature Formats* and GlobalSign/ICRI, *Signature Policies*, 28 August 2000.

[21] On the other hand it is envisaged that the user's local system will check the applied policy in connection with the verification of the signature, e.g. by checking against the list of accepted policies.

represented in the system in the correct manner, and that processing can be implemented legally without manual processing. The implementation of such quality assurance and approval must be a mandatory requirement and cannot be subject to negotiation when contracts relating to the development or supply of information systems are entered into.

When the final remains of manual case processing are lost from an area, we also lose our grasp on the idea of case officers who make well-considered decisions. Our Public Administration Act is probably based on this assumption.

A considerable amount of automation is already undoubtedly occurring in some areas of public administration today. However, up until now, this has to a certain extent been "concealed" behind the routines for the sending of information on paper, which has occurred irrespective of the form of processing used. Now that we are progressing towards an ever-increasing degree of electronic case processing and electronic communication, this hallmark of traditional case processing is also disappearing. It may therefore be time to consider whether the Public Administration Act should expressly allow for fully-automated decision-making processing and at the same make the requirements relating to such systems transparent by arranging for or authorising the drawing up of requirements relating to quality assurance and approval.

11.2.5.4 Issue and use of certificates for information systems

The above sections provide the background for the following proposals:

- Information systems which are used in connection with fully or partially automated processing, and which produce results which are or emerge as being decisions in the sense of the Public Administration Act, should be equipped with certificates which identify the department for which the information system processes messages.
- Thecertificate should contain information providing confirmation to the recipient of the message about the link which exists between processing carried out by the information system and the department concerned.[22]
- The recipients of messages linked to such certificates can consider such messages as though they were signed by someone working for the public administration having authority to deliver or sign such messages or decisions, unless the person concerned knew or should have known that the message or decision concerned was the result of an error.[23]

---

[22] This can, for example, occur if a certificate contains information which, when shown on a recipient's screen when using ordinary software, appears as the department's commonly recognised name. If the department uses several information systems, each individual system should be equipped with its own set of keys and certificates.

[23] It is not intended that this should interfere with the opportunity which otherwise exists to put aside or reverse decisions which are encumbered with errors – only the fact that the decision has not been made by the right person within the relevant agency. In principle certificates can also be envisaged for public administration employees which do not contain the employee's name, but on the other hand have the name of the public administration agency along with an employee number or other identificator which will enable the agency to identify the case officer. Unless the case officer's name appears elsewhere on the message, the case officer will be anonymous for the recipient. It is then envisaged that the same legal effect would occur as that which exists for messages "sealed" by the agency's information system. However, there is no automated processing or other circumstances here which would justify the special transfer of risk of error to the public administration agency. Therefore, there appears to be no reason to treat users of any "anonymous certificates" any differently to when case officers sign their full name.

- Applications relating to the issue of certificates which link signature-verification data (public key) to an information system and a government department, and which are to be used during processing which can result in decisions in accordance with the Public Administration Act, should be approved by whoever is authorised to issue authorisation on behalf of the department concerned.

11.2.5.5 Observations relating to vulnerability – securing keys for information systems

Those public administration systems which have to be equipped with their own certificates for signature/sealing, must mainly be assumed to be activity critical systems. Breakdowns in or "attacks" on such systems would paralyse activities for a while.

If the key certificate for such a system is revoked, the system will in practice be put out of operation because it would no longer possible to verify messages from the system. It is not likely to be an insurmountable problem for some people to wait a day or two for new keys and a new certificate, if the signature key should become compromised. For larger enterprises, such as public administration agencies, even a breakdown lasting a few hours could be critical. Unless the generation of new keys and issue of a new certificate can be carried out rapidly, routines should therefore be established so that such information systems are equipped with at least one extra set of signature keys which can be employed rapidly if a certificate is revoked or a signature key is lost, e.g. as a result of technical failure.

The consequences of system breakdowns also constitute a particular challenge in respect of the vulnerability which lies in the possibility of keys used by certification service providers for signing certificates, being compromised. If such keys are compromised, the basis of trust is snatched away in respect of all certificates issued by that certification service provider with the key in question.

In the latter case, having several keys from the same certification service provider will not help since they all would be exposed to the same break down in trust. It should therefore be considered whether or not information systems for public administration agencies should be equipped with keys (signature generation data) from at least two independent certification service providers.

Signature keys used in automated systems must be installed so that they can be used directly by the system concerned without any human intervention. This makes demands on securing information systems in order to avoid the misuse of, and attacks on, the keys in question. Since security measures cannot be based on individual approval of each individual "signature," c.f. what is said about usage by public administration agency employees in footnote 27 below, measures must instead be linked to physical and logical securing of information systems and the environment in which they operate.

- As regards an information system which is equipped with certificates for public administration agencies, routines should be drawn up designed to ensure that the system in question can be put into operation rapidly with new

signature generation data and a new certificate if the certificate which is being used is revoked or if signature generation data is lost.
- It should be considered whether or not information systems should be equipped with signature generation data and certificates from more than one certification service provider.
- Signature generation data should be secured against misuse in accordance with recognised principles relating to the security of information systems.

11.2.6 Use of electronic signatures by public administration employees

11.2.6.1 Procurement of keys, codes and certificates

In order to be able to implement electronic case processing on a large scale, employers must be able to instruct thepublic administration employees to make use of the security services which the public administration agency in question has chosen to use in respect of case processing. The manner in which the allocation of keys, codes and certificates takes place, and where individuals will need to make enquiries about registration, etc., will be depend on which service(s) has/have been selected. Employers will therefore have to provide the public administration employees with instructions as to how they should proceed.

For coordination purposes, and in order to secure maximum efficiency in respect of internal public administration communication processes, certificates to be used by public administration employees in the course of their employment should only be issued by certification service providers which the public administration agency, or the coordinating body for the public administration, has appointed/approved and, possibly, entered into a framework agreement with.[24] This makes it possible *i.a.* to secure interoperability and access to necessary certificate catalogues, to ensure that all public administration employees have access to those certificates[25] which are necessary for certifying other civil servants' certificates, and to check that services maintain a satisfactory security level. If it is necessary for coordination purposes, or because some public administration agency lacks expertise in the relevant area, it may be expedient to limit the choice of certification service providers with whom framework agreements have been entered into. It is assumed that the system of framework agreements will have been organised in accordance with the regulations relating to public procurement.
- A public administration agency can provide its employees with instructions about which security services they should use while working for the agency concerned, and where they should apply or how they should proceed in order to obtain necessary keys, codes, certificates, etc.
- In the course of their employment, public administration employees shall only use certificates issued by certification service providers who are approved by their employer or by a public administration agency which is responsible for coordinating the public administration's activities.

[24] A solution should be sought which would make it possible to coordinate both central and local government administration.
[25] The certificates of the relevant certification service provider.

- Coordinating public administration agencies can decide that, while working for a public administration agency, only certificates issued by certification service providers, who have entered into a framework agreement relating to the supply of such services to the public administration, can be used.
- If the framework agreement expires and is not renewed during the term of the certificate's validity, it should nevertheless be possible to use the certificate for the remainder of the term of validity, unless the certification service provider's certificate is revoked, or the necessary catalogue services, etc., are no longer available.
- Coordinating public administration agencies can decide that such certificates should nevertheless not be used after a framework agreement has expired.[26]

11.2.6.2 What needs to be documented when procuring a certificate?

Those matters which need to be documented when procuring keys, codes or certificates, etc., will depend on which security solution has been chosen. For employee certificates, it will normally be enough to document the user's identity and employment. For other types of certificates, it may in addition be necessary to provide information about the authority and professional links, etc. of the person concerned.

Routines and requirements relating to documentation in connection with the procurement of certificates will appear on the certificate or signature policy chosen by the public administration agency concerned, and which a certificate is to be issued in accordance with.

11.2.6.3 Collection of information and consentfor certificate delivery, etc.

In accordance with the draft Act relating to electronic signatures [52], information which is to be used on certificates can only be obtained directly from the person to whom the information relates, or with his/her express consent, cf. Section 7.

Furthermore, certification service providers cannot deliver certificates to others without the certificate holder's consent, c.f. (presumably) sub-paragraph (b) of the second paragraph of section 14 of the Act relating to electronic signatures. If public administration employees are to be allowed to sign outgoing messages themselves, consent will need to be obtained for delivering such certificates.

It is hardly practical or tenable that the recipient of a message, signed by a public administration employee in service, is unable to access the relevant certificate. If such consent is not given, the consequences of this should be that the employee concerned would be unable to engage in external electronic case processing.

Under normal circumstances the relevant certificate will be appended to the message so that it is not necessary for the certification service provider to deliver it. However, one should not exclude the possibility of obtaining certificates directly from the provider (or even the web site of the public administration agency concerned), and consent should consequently be obtained on a routine basis. Certificates which are to be used in connection with encryption (using the recipient's public key) must be

[26] If it were not possible to ensure full support for certificates up to the time they expire, it must be possible to demand that use is discontinued during the period of validity.

obtained from the certification service provider if the sender was not previously familiar with the certificate. However, such certificates are not covered by the Act relating to electronic signatures.

- The collection of information to be used on a certificate shall be obtained directly from the person to whom the information relates, or with his/her express consent, cf. Section 7 of the Act relating to electronic signatures [52].
- In connection with applications from public administration employees relating to certificates for use in service, the certification service provider shall request the employee's consent for the delivery of such certificates to others, cf. (presumably) sub-paragraph (b) of the second paragraph of section 14 of the Act relating to electronic signatures.
- At the same time, one should seek consent for handing over information about an employee's duties or authority in service when such information is stored in linked catalogues and not directly in the actual certificate, provided that such information can be expected to be relevant to the use of the certificate. It shall only be possible to give out such information in connection with the verification of the relevant certificate.[27]

11.2.6.4 Guidance for employees

Because little is known about the use of electronic signatures, etc., it is important that adequate and suitable information is given to the user before the techniques can be employed.

When procuring keys, codes and certificates, employees shall receive information/guidance about:

- Responsibilities and obligations in connection with the storage and use of keys, codes and certificates, etc.,
- Current certificate policy and practice (in the form of an adapted user version),[28]
- Their own and others' opportunities to blacklist or suspend certificates,
- Expiry of certificates,
- Certification service providers' storage of personal information, storage periods and to whom the certificate can be delivered, etc., cf. Section 19 of the Personal Data Act,
- Responsibilities and obligations of certification service providers,
- Responsibilities and obligations of the registration authority,
- Restrictions on the use of certificates.

11.2.6.5 Instructions relating to the use of keys, codes and certificates

[27] The idea is that it should not be possible to "surf" through the catalogue in order to map an individual's authority, but only in order to receive verification whether the person concerned possesses the necessary rights or is connected to the relevant area in respect of the use of the certificate.

[28] It is important that this information is provided in a form which the user can understand. It cannot be expected that individuals would be capable of relating directly to current certificate policy and certification practices. See, for example, *Model PKI Disclosure Statement* (PDS) in ETSI TS 101 456, *Policy Requirements for Certification Authorities Issuing Qualified Certificates, Annex B*.

As assessment should be carried out into whether public administration agencies and public administration employees should be obliged to use digital signatures or the equivalent in certain contexts.

When public administration agencies draw up criteria for when case officers should use digital signatures, etc., the criteria should, as far as possible, be linked to assessments which the case officer in question is, in any case, supposed to undertake, e.g. assessing whether a message which is to be filed in accordance with the Archives Act is covered by the finance regulations, or whether it concerns a *decision* in the sense of the Public Administration Act. This can apply to both decisions relating to material issues and procedural decisions, e.g. about rejecting a complaint or enquirywhich would otherwise involve a case being initiated. As far as possible, one should avoid introducing new assessment issues for individual case officers.

If a solution with central "sealing" is chosen for messages and notification about decisions over dedicated information systems, the need for imposing duties on individual case officers in respect of signature will be considerably reduced.

11.2.6.6 Other use of keys, codes and certificates

Apart from those cases where there is an obligation to use digital signatures or to send messages via a communications centre, case officers should themselves be able to chose whether to use digital signatures during the course of their duties when they consider it to be expedient, or if a recipient so demands.

11.2.6.7 Restrictions on the use of keys, codes and certificates

In order to avoid a confusion of roles, the Committee has decided that it would be most expedient if personal certificates (employee certificates) which contain links to a public administration agency as the employer, are not used for purposes other than those which relate to duties carried out for the employer in question. For private purposes, individuals must obtain a personal certificate.

- Authentication data or certificates (e.g. employee certificates) which contain links to a public administration agency in its capacity as an employer shall only be used to carry out duties for the employer in question.
- Personal (private) certificates should not be used when carrying out duties for an employer.

11.2.6.8 Requirements relating to the proper use and storage of keys/key-bearing media

Irrespective of which solution is chosen for individual use, requirements need to be stipulated in respect of the individual's association with, and the use of, signature-creation devices (signature keys) or authentication data (passwords/PIN codes). This is a prerequisite if people are to have trust in the solution.

This means, first of all, ensuring that no-one else acquires access to codes and keys, secondly that codes and keys are only used for the purpose for which they are issued,

and thirdly, owners must never leave their computer unsecured in such a state that someone else could continue an active session or send messages on behalf of others.

In addition, there is a need to ensure that signature-creation data, and the data which is to be signed, are not "attacked" or "misused" by the information system in which they are used, e.g. as a result of a virus, etc. This places demands on the signature-creation device, the user's other system configuration, the surrounding environment ("firewalls," etc.) and PCs as such. Such demands must initially be dealt with by the unit which is responsible for the procurement and operation of the enterprise's information systems, c.f. point 11.4. Users must then be instructed not to undertake any actions which could threaten the security of the system, such as uncritical downloading or the installation of non-approved software, etc. In practice this will probably need to be resolved by the employer providing instructions about the use of the enterprise's information system.

- Owners of signature-creation data shall store and use such so that it does not become available to others.
- Signature-creation data shall only be used for the purposes for which it is issued.
- Owners shall never leave their workstations, terminals or other units which are used for authentication or signature generation without ensuring that signature-creation data is no longer accessible on/in the unit, that the current session has been concluded, or that the unit has otherwise been secured against misuse by a third party.[29]
- Owners of signature-creation data shall not entrust it to others or give others access to it, not even when others are going to act on their behalf. If someone is going to act on behalf of another party (with authority), this shall occur with the authorised representative's own signature-creation data with reference to the fact that the message has been submitted on behalf of someone else. (The person for whom someone acts on behalf of can issue a role certificate to his authorised representative (when this becomes available)).
- The provisions relating to signature-creation data apply likewise to the use of authentication data (passwords/PIN codes).
- Employees shall otherwise follow the instructions laid down by their employer relating to the use and security of the enterprise's information system, including information about controls on material which shall be downloaded or installed in the information system.

11.2.6.9 Notification obligations re. loss of keys, suspicion of misuse, etc.

The proper use of codes, passwords, keys and key-bearing media involves immediate notification if it is suspected that keys have been lost, have gone astray, or are otherwise being, or could be, misused.

- The owner of signature-creation data or authentication data should immediately notify the certification service provider or the person who has been appointed to receive such notification if signature-creation data or

[29] A number of problems are resolved if the access password for signature keys has to be given each time the signature key is to be used, as proposed in Sweden. However, unless signature takes place in active cards, etc., this would probably be dependent on the individual's local configuration.

authentication data are suspected to have been lost, to have gone astray or are otherwise being, or could be, misused.

11.2.6.10 Requirements relating to the control of certificates and revocation lists

When receiving messages equipped with a signature, there should *inter alia* be checks carried out to ensure that the signature can be verified, that the relevant certificates are still valid and satisfactory for the relevant application, that the certificate belongs to the correct person, etc. The checks that should be carried out and the additional information that should be obtained will depend on which service is used, and how critical the application in question is. These requirements can be defined under a signature policy.[30]

The question relating to the extent to which case officers should carry out the relevant checks is dependent on which services exist centrally at the agency concerned and which functions are automatically carried out by local workstations, cf. verification of signatures on receipt under point 11.2.5. However, these are tasks which should be resolved automatically as far as possible. On the other hand, if verification is not successful, and this means that further processing of the message cannot be carried out, the case officer must initiate a message to the sender in accordance with the rules relating to messages which fail to satisfy the requirements mentioned under point 11.3.5.[31]

- If a message equipped with an electronic signature cannot be verified in accordance with the rules which apply to the type of message in question, and if this is important for a public administration agency in processing the message, a message should be sent to the sender in accordance with the rules mentioned under point 11.2.3.

11.2.6.11 Requirements/recommendations relating to local storage of certificates, etc.

Information necessary for verifying a signature should be stored along with the message or by maintaining a local certificate database and blacklist, etc., and with reference to the specific message concerned. In addition to the relevant certificates, this information can also serve, for example, as confirmation of checks made on revocation lists, etc. Such information should be stored in the archives, as far as possible, or be replaced by the archives' confirmation of those matters that have been verified, cf. that which is said about archives and long-term storage in point 11.2.4. If a message is temporarily stored somewhere other than in the central archives, the agency or case officer's local system is to attend to this task.

- Copies of relevant certificate(s) and other information necessary for verification of signatures over time should be stored in the archives.

---

[30] Cf. for example, ETSI ES 201 733 Electronic Signature Formats and GlobalSign/ICRI, *Signature Policies*, 28 August 2000.

[31] It is not certain that a lack of verification will always be important for the processing of the message. For example, it might be the case that a message concerns a request for access to a document which can be submitted in accordance with the Freedom of Information Act, or a request to be sent an application form or other matters where the identity, etc. of the person concerned is irrelevant.

- If a message is stored locally temporarily by the user, without being sent to the archives, information to this effect should be stored locally together with the message.

11.2.7 Use of electronic signatures by private persons

The public administration has an obvious interest in, and need for, clear rules relating to the handling of electronic messages that are received, processed and sent by public administration agencies. On the other hand restraint should probably be displayed in imposing obligations on citizens as to how they should deal with messages in their own information systems. With the exception of those measures that are important for communications between the public administration and individuals, guidelines aimed at citizens should probably be in the form of recommended guidelines rather than binding rules.

The manner in which messages are handled by the public administration and citizens will have a number of common features, and the questions being treated will largely be the same. However, solutions may vary, partly because individuals do not normally have access to communications centres which verify signatures or archive functions which are able to undertake long-term storage of electronic messages in a satisfactory manner. It is possible that individuals ought perhaps to be able to base themselves on the public administration's archives in respect of the long-term storage of messages which have been exchanged with a public administration agency.

11.2.7.1 Choice of security service

As a point of departure, there should be no restrictions relating to citizens' access to freely choose which certification service provider they will use, provided that the service satisfies the requirements imposed by the public administration agency concerned. However, it may be necessary for those who have not already acquired keys and certificates, etc. to use a certification service provider who has been appointed or is operated by the public administration agency concerned or its coordinating body. In such cases users do not need to undertake an independent assessment as to whether or not the service has a satisfactory level, but can base themselves on the assessments which have already been carried out by the public administration.

Freedom as regards the choice of certification service providers causes problems in respect of where/to whom individuals, in their capacity as private persons, should apply in order to apply for a certificate. If a public administration agency has issued instructions about satisfactory services, cf. above, it will normally explain where and how one should proceed when making a choice between the services specified.

- When engaging in electronic messages with the public administration, individuals must use services which comply with stipulated requirements.
- If qualified signatures are used, individuals may make their own choice about which supplier of qualified certificates they wish to use.
- The public administration may stipulate additional requirements within the framework of Section 5 of the Act relating to electronic signatures.

11.2.7.2 Guidance for users

Because most users are currently unfamiliar with the use of electronic signatures, etc., it is important that adequate and proper information is provided to users before the techniques are used.
When procuring keys, codes and certificates, users should receive information/guidance about:

- Responsibilities and obligations in connection with the storage and use of keys, codes and certificates, etc.
- Current certificate policy and practice (in the form of an adapted user version),[32]
- Their own and others' opportunities to blacklist or suspend certificates,
- Expiry of certificates,
- Certification service providers' storage of personal information, storage periods and to whom certificates can be handed over, etc., cf. Section 19 of the Personal Data Act,
- Responsibilities and obligations of certification service providers,
- Responsibilities and obligations of registration authorities,
- Restrictions on the use of certificates.

11.2.7.3 Restrictions on the use of keys, codes and certificates

There is reason to assume that the public administration will accept and use a number of those certification services which are otherwise available on the market. These services may have a general application or be recommended for use in one or more specified areas by the certification service provider. There is not really any need to get into this.

If on the other hand it should become necessary to issue certificates or other authentication data exclusively for use in communications with the public administration, legal basis should exist to direct the user to respect such. To avoid uncertainty, such restrictions should appear on the certificate, and the attention of the user must be drawn in particular to such restrictions.

- Signature-creation data or authentication data which is assigned to individuals especially for communication with the public administration should not be used for other purposes.
- Such restrictions should appear on the certificate and the user should be informed about them, cf. the above guidelines.

11.2.7.4 Requirements relating to the proper use and storage of keys/key-bearing media

[32] It is important that this information is provided in a form which the user can understand. It cannot be expected that individuals should be able to relate directly to current certificate policy and certification practices. See, for example, *Model PKI Disclosure Statement* (PDS) in ETSI TS 101 456, *Policy Requirements for Certification Authorities Issuing Qualified Certificates*, Annex B.

Irrespective of which solution is chosen for individual applications, requirements must be specified for the individual handling of and use of signature-creation data (signature keys) or authentication data (passwords/PIN codes). This is a prerequisite for having trust in the solution concerned. This means, first of all, ensuring that others do not gain access to codes and keys, and secondly that codes and keys are only used for the purpose for which they are issued. This should apply in general to all use of security services.

As far as employees of the public administration are concerned, there is an additional requirement that they should never leave their computers unsecured in a status where others could continue an active session or send messages on behalf of another. It is doubtful whether the latter type of restriction can or should be imposed on private persons unless keys, codes or certificates are issued specifically for use with the public administration. On the other hand, definite encouragement should be given to follow the same rules.

It will also be necessary for individuals to ensure that signature-creation data and data which is to be signed is not "attacked" or "misused" by the information system in which it is used, e.g. as a result of viruses, etc. This places demands on the signature-creation device, the user's other system configurations and the surrounding environment ("firewalls," etc). Private individuals will normally have to rely on their system supplier in these matters. It will subsequently be up to the user not to engage in actions which could threaten the security of the system, e.g. uncritical downloading or the installation of non-approved software. Even though a lack of follow-up on the part of the user can result in faults or misuse, and subsequently in general pressure on trust in the signature system, one should probably be careful about imposing restrictions on individuals' access to procure and make changes to their own systems. On the other hand, recommendations should be provided, preferably by certification service providers, about how individuals should proceed. For applications where the security requirements are high, it is probably a good idea if the use of so-called "secure signature generation devices" is demanded, c.f. Chapter II of the Act relating to electronic signatures, or that other special demands are placed on the user's information system.

- Owners of signature-creation data shall store and use it so that it is not accessible by others.
- Signature-creation data shall only be used for the purposes for which it is issued.
- The owner of signature-creation data should never leave his/her work station, terminal or other unit used for authentication or signature generation without ensuring that the signature-creation data is no longer available on/in the unit, that the current session has been concluded, or that the unit has otherwise been secured against misuse.[33]
- The owner of signature-creation data shall not entrust it to others or provide others with access to it, not even when others are going to act on his/her behalf. If someone is going to act on behalf of another party (with authority), this should occur with the authorised representative's own signature-creation data with reference to the fact that the message has been delivered on behalf of

[33] A number of problems are resolved if the password for access to the signature keys has to be given each time a signature key is to be used, as proposed in Sweden. However, unless signature takes place in active cards, etc., this would probably be dependent on individuals' local configuration.

someone else. (The person for whom someone else acts on behalf of, can issue a role certificate to his authorised representative (when this becomes available)).

- Similarly, the provisions relating to signature-creation data apply to the use of authentication data (passwords/PIN codes).
- Owners of signature-creation data should only use it in information systems which they have confidence in, and follow the recommendations given by the certification service provider about adjusting and using the system. Caution should be displayed if changes are made to the system, and one should check material which is to be downloaded or installed in the information system.

11.2.7.5 Notification obligations re. loss of keys, suspicion of misuse, etc.

The proper use of codes, passwords, keys and key-bearing media involves immediate notification if keys are suspected to have been lost, to have gone astray or are otherwise being, or could be, misused. This applies irrespective of who the owner is.

- The owner of signature-creation data or authentication data should immediately notify the certification service provider or the person who has been appointed to receive such notification if signature-creation data or authentication data are suspected to have been lost, to have gone astray, or are otherwise being, or could be, misused.

11.2.7.6 Requirements relating to the control of certificates and revocation lists

When receiving messages equipped with a signature, it should *inter alia* be checkedwhether the signature can be verified, whether the relevant certificates are still valid and satisfactory for the relevant application and whether the certificate belongs to the correct person, etc. The checks which should be carried out and the additional information which should be obtained will depend on which service is used, and how important the application in question is. These requirements can be defined in a signature policy.[34]

Unlike public administration case officers, who can have the function covered by a centralised service, individuals must see to the necessary verification themselves. These tasks should, as far as possible, be resolved automatically. The most important of these functions will probably be available and automated in individuals' local information systems and through their service suppliers. Individuals cannot really be asked to do this manually. Any guidelines must therefore contain recommendations which are levelled at both the suppliers of products and services and users themselves.

If, on the other hand, verification is not successful and this means that further processing of the message cannot be carried out, the user must initiate a message to the sender in the same way as a case officer in an administrative agency would.

- If a message which is equipped with an electronic signature cannot be verified in accordance with the regulations which apply to the type of message in question, and if this is important for the processing of the message, a message should be sent to the sender.

[34] Cf. for example, ETSI ES 201 733 *Electronic Signature Formats and GlobalSign/ICRI, Signature Policies*, 28 August 2000.

11.2.7.7 Requirements for/recommendations on local storage of certificates, etc.

Information necessary for verifying a signature should be stored along with the message or by maintenance of a local, historical certificate database and blacklist, etc., and with reference to the individual message concerned. In addition to the relevant certificates, such information can also serve, for example, as confirmation of checks made on revocation lists, etc.

Contrary to that which applies to the public administration, individuals will not normally have access to archive services which can maintain this function. It is also difficult to see how individuals could manage this by themselves. It may therefore be necessary to allow individuals to base their long-term storage of messages exchanged with the public administration in the agencies' archives. This would further serve to reinforce the need for the public administration to comply with the obligation to log and file records. During the period when an actual transaction or the exchange of information takes places, individuals should also store the necessary information themselves. It is also possible that special services will emerge which will provide storage facilities for electronically stored material over time.[35]

- Storage of relevant certificate(s) and other information necessary for the verification of signatures which are used when communicating with public administration agencies is something which individuals can entrust to the public administration's archives.
- The manner in which long-term storage and delivery to individuals will occur is subject to the regulations which apply to the archives at any one time.
- During the period when an actual transaction or the exchange of information takes place, individuals should also store the necessary information themselves.

11.2.8 Intervention re. misuse of certificates in communications with the public administration

Electronic case processing must build on trust in the security systems chosen. However, security is dependent on users behaving with due care and in good faith. If a number of users misuse a security system, this will undermine confidence in the system as a whole. It should therefore be possible to deny access to users who misuse the system. Denial of access can occur, for example, by blocking the user name, or by revoking certificates.

This may be a matter for the individual certification service provider, but could also apply directly to public administration agencies, either because the agency itself administers codes or passwords, or because the agency no longer has reason to have trust in the user of a particular certificate. In such cases, blacklisting can be undertaken either by the certification service provider, if the relevant policy allows for

[35] See, for example, SINTEF's preliminary project relating to a "Nasjonal BitBank" in the report entitled *Langtidslagring av informasjon. Underlag for etablering av en BitBank* (Long term storage of information. Basis for the establishment of a BitBank), SINTEF Report STF40 A99082, 28 December 1999.

denial of access in accordance with initiatives taken by third parties or the certification service provider itself, or in the public administration agency's own local blacklist, if such exists. Using such "internal lists" should be considered as part of the local key administration policy if citizens are free to choose certification services supplied by other providers than those with whom the public administration has an agreement.

If a citizen uses a certificate supplied by an independent certification service provider, which can also be used for purposes other than communication with the public administration, it is not certain whether any misuse in connection with, for example, reporting to the public administration, will provide grounds for revoking the certificate as such, since revocation will also deny access for other applications. There could, however, be grounds for the public administration agency to blacklist the certificate for use with such agency. This could be done by using local blacklists, or by coordinating with batches of downloaded blacklists from certification service providers. A solution of this type would be less of an encroachment on the certificate owner than the inclusion of a certificate on the certificate service provider's blacklist.

At the same time, one should make allowances for the fact that the denial of access through blacklisting of codes or certificates could have an encroaching effect on individuals. Routines must therefore be set up for the quality assurance of information which forms the basis of such decisions, for access to review, for the handling of certificates while complaints are being dealt with, and for routines which ensure that such processing takes place quickly.

Before blacklisting takes place, certificate holders must be allowed the opportunity to have their say. Since the blacklisting of a certificate is presumably a reaction to a gross breach of trust displayed by a certificate holder towards the public administration agency, and as continued misuse could cause the public administration or others loss or extra work, the deadline should not exceed the period necessary for a certificate holder to submit objections against blacklisting of a certificate.

- In the event of proven suspicion relating to the misuse of a certificate when communicating with a public administration agency, the agency concerned can blacklist the user's identity or certificate in respect of further use with that agency. The same applies if a certificate owner abuses his permission or access to communicate electronically with the agency concerned.[36]
- Before a certificate is blacklisted, the public administration agency concerned shall notify the certificate holder that they are considering blacklisting the certificate, and their reasons for doing so. The certificate holder should be encouraged to state his opinion on the grounds forblacklisting. The public administration agency shall set a deadline for receipt of such statements (which shall not be less than (number) days).
- If, after having considered the certificate holder's comments, the public administration agency decides to blacklist the certificate, it should send notice to this effect immediately to the certificate holder.
- The certificate holder can appeal against a decision to effect blacklisting.

[36] For example, in the event of systematic fault reporting to an automated reporting system.

- Appeals relating to the blacklisting of certificates should be processed as rapidly as possible, and the appeal body can decide that an appeal shall bepostponed.
- The administrative appeal body dealing with the blacklisting of a certificate shall be appointed by the King/coordinating ministry. Special regulations may be laid down relating to the processing of appeals relating to the blacklisting of certificates.
- Such provisions shall apply similarly to the blacklisting of authentication data (user name and accompanying password/PIN code) in information systems arranged by a public administration agency where such are suitable.

11.2.9 Copy of signature keys

Copying signature keys for private individuals and employees should not normally occur. If a signature key goes astray, it will be possible for others to act as the holder's "electronic double" until the accompanying certificate has been blacklisted.

Nor is there any great requirement for signature keys to be copied. If a key is lost or goes missing, a new one can be generated and a new certificate can be issued. Being without a key and certificate during the period of re-issue is hardly likely to present private persons with insurmountable problems.

Data will not be lost even if a signature key is lost or a certificate is suspended. The problems associated with the verification of signatures with revoked certificates are discussed in point 11.2.4 about archives.

See point 11.2.5 for stand-by solutions for automated systems.
- Signature keys issued to individuals shall not be copied.

11.3 Content encryption and handling of keys

11.3.1 Introduction

Requirements relating to content encryption[37] (the securing of confidentiality) are in part actuated by other rules and are based on considerations other than requirements for the securing of integrity, authentication and non-denial. There are other requirements for users regarding content encryption. If is therefore considered appropriate to deal with these issues separately – *inter alia* to avoid confusion.

When the final rules have been drawn up, coordination with the rules relating to electronic communication and signature services can be considered. However, such coordination would be conditional on 1) a simplification or other improvement in efficiency of the regulatory framework, and 2) there being no risk of

[37] Content encryption here means a measure for ensuring confidentiality, etc., not encryption of content in connection with systems for pay-TV, rights administration, etc.

misunderstandings. Otherwise it would probably be better to keep the rules separate, at least in the different chapters in the same regulations/instructions. Simplifications could, for example, be linked to joint procedures for applications and the processing of applications relating to the issue of keys, cards, codes and certificates. Misunderstandings could occur, for example, as result of confusion of terms.

The use of content encryption places demands on both employees working for the public administration and individuals who communicate with the public administration. This applies to the proper treatment of keys, the choice of the right key for encryption (possibly by a session key), routines for the reception of encrypted material and back-up copies, storage or deposit of encryption keys. The requirement relating to availability is conditional on solutions which ensure that material is not lost as a result of keys being lost or destroyed.

The recommended rules do not interfere with the rules which actuate requirements relating to the use of content encryption or other methods of securing information, but are meant to serve as a supplement which can be employed when encryption or security measures are to be used.

11.3.2 Coordination of requirements relating to content encryption

Requirements relating to or the need for content encryption can be actuated from several quarters: first through general rules relating to the obligation of confidentiality, c.f. Section 13, etc. of the Public Administration Act and similar provisions contained in special legislation relating to the public administration. Secondly, through requirements relating to the processing of personal information, c.f. Section 2 no. 8 of the Personal Data Act and the draft regulations relating to the securing of personal data (now Chapter 4 of the draft regulations relating to the Personal Data Act). Thirdly, documents classified according to the protection instructions (or the Security Act and its appurtenant regulations). Finally, through the public administration's need to secure information exempt from publication in respect of other considerations than those which apply to the above mentioned regulations – e.g. processing budgets, etc.

It would obviously be an advantage to achieve as much coordination as possible in respect of the requirements relating to content encryption actuated by the rules relating to the duty of confidentiality, the processing of personal data and other internal administrative requirements.

In many cases the duty of confidentiality will be linked to the processing of personal data – and the processing of personal data presumably forms a normal part of the communication that takes place between the public administration and citizens, at least as regards case-related information.

Unless a need for special security requirements can be established in respect of the areas covered by the relevant public administration agencies, e.g. the health service, the national insurance service and the social welfare service, which may involve more stringent requirements, one should aim at operating with a common security level

that is suitable for all three of the cases previously mentioned. This could involve "over-fulfilment" of the requirements, but this is nevertheless preferable, because those involved will be subject to security requirements on a regular basis which are governed by more than one set of regulations, and it would be difficult for individual case officers (or reporting centres) to assess security requirements in individual cases.

It is otherwise likely that to envisage that the protection of sensitive personal data will represent an outer limit for what is required, also in respect of general confidentiality.

11.3.3 Information for citizens when transfering personal data and confidential information to the public administration

The obligation of the public administration to secure information in accordance with the rules relating to the duty of confidentiality and the processing of personal data should, if nothing more than an expression of their duty to provide guidance, activate a duty to inform citizens about the risks associated with the electronic transfer of (personal) data, and to make arrangements so that citizens can easily gain access to the appropriate security services.

Confidentiality and the rules on processing normally apply to public administration agencies as such. Individual citizens can undoubtedly decide if they themselves want to send unsecured information to the public administration. However, such decisions should be based on relevant and adequate information so that the person concerned can make an "informed" decision. If the public administration agency concerned actively makes a communications channel available which involves a risk to users, this will probably lead to a tightening up of the duty to provide guidance, so that individuals can more easily look after their interests.

Such an obligation must be limited to those cases where the public administration is actually in contact with the party concerned before information is transferred, e.g. if the party concerned visits the relevant website, downloads a suitable form or otherwise gains access to information which states or gives the impression that information can be sent electronically. It would be difficult to do anything about the transmission of initial e-mail messages containing personal information or other information which the public administration is bound to keep confidential.

- A public administration agency, which sets up its systems to receive information from individuals or organisations, which information it may be required to keep confidential or which is subject to security requirements in accordance with the rules relating to the processing of personal information, shall inform the individual concerned in a suitable manner about any risks involved in the electronic transmission of the information concerned.
- The public administration agency shall make necessary security services easily accessible to individuals, or provide information which makes it easy for individuals to gain access to such services.
- The public administration agency shall also (on request) provide information as to how personal data or confidential information is secured while being processed by the agency concerned.

- If the risk of unauthorised access to confidential information or personal data cannot be easily prevented by the individual concerned, the public administration agency shall not communicate in this manner.

11.3.4 Procurement and use of keys, cards, codes and certificates, etc.

The rules relating to individual procurement of keys, cards, codes and certificates should mainly follow the same rules which apply to electronic signatures. The same applies to requirements relating to the proper handling of keys and codes, as well as requirements relating to notification in the event of loss or suspected loss or misuse.

11.3.5 Encryption of messages sent to the public administration

In most cases, messages sent by individuals to a public administration agency will concern the agency in question and not just an individual case officer. Nor will individuals usually know which case officer they should send a message to. Under normal circumstances, messages sent to a public administration agency should therefore use a common encryption key relating to the public administration agency concerned. Subsequent protection of messages must be undertaken by the public administration's system in accordance with the rules on how to process that particular message.

As regards certain types of material, it is nevertheless possible that there will be a need to ensure confidentiality all the way to the case officer. This may apply, for example, to information relating to child welfare or social welfare matters to which just one or a few case officer(s) shall have access. It should therefore be possible to make exceptions to the rule about using keys linked to the agency concerned, even if such a rule may also vary, e.g. to a department, etc.

Messages addressed directly to a case officer, encrypted using the case officer's public key, are conditional on special internal routines, e.g. as regards the handling of keys in the absence of the case officer concerned and questions relating to the deposit of copies of employees' encryption keys, etc. It should therefore be up to the individual agency concerned to make arrangements in this respect, c.f. what has been said about direct addressing and management under points 11.2.3 and 11.3.8.

- When encrypting a message sent to the public administration, an encryption key linked to the public administration agency concerned should be used.
- Encryption using an encryption key linked to a case officer can only be undertaken if the agency concerned has set up its system for this.

11.3.6 Restrictions on use

Restrictions should not be placed on the use of private individuals' encryption keys unless a particular need can be established for them.

11.3.7 Receipt of encrypted material

Material which has been received should be decrypted on receipt. This will *i.a.* ensure that the material is actually available to the agency concerned. While it is encrypted, it is also difficult to check to see whether a message is virus-free, etc. The message should be checked before it is disseminated around the organisation's information system. If decryption fails, the sender should be notified that the public administration agency is unable to access the message, and which measures he/she should implement. Usually, it will simply be a question of re-sending the message.

The protection of data in an agency's own internal system can occur by other means than encryption against the outside world because the "rules" relating to access to and use of the system are defined by known participants and the public administration agencies themselves.

- Messages received by public administration agencies in encrypted form shall be decrypted immediately.
- If it is not possible to decrypt a message on receipt, the message should be returned to the sender immediately with a message, stating that it was not possible to decrypt the message (not accessible by the public administration agency or other recipient), and that a new message should be sent.
- Messages returned on this basis should be recorded/logged by the public administration agency along with information about who the sender was, the time when the message was received and returned, and a description of the contents of the message, if known (e.g. by looking at an open title, etc.).
- For messages which are returned because they are not accessible for the public administration agency concerned because a different encryption key has been used than the one specified by the agency (or because the contents of the message are not accessible to the public administration agency for other reasons), the provisions contained in the Public Administration Act relating to rejection and redress shall apply.
- The protection of data in an agency's own internal system takes place using the tools which the agency or coordinating agency concerned has decided are necessary and suitable.

11.3.8 Deposit or other back-up copies of encryption keys

It is obviously important that material should not become inaccessible to a public administration agency because encryption keys have been lost. It may therefore be necessary to stipulate requirements relating to back-up copies and/or the deposit of encryption keys.

There are objections from a privacy point of view as regards a requirement for back-up of copies and the deposit of encryption keys. However, if requirements are established to the effect that one should use encryption keys linked to a public administration agency (and not a case officer) when encrypting material to the agency, and the requirement relating to copying/storage or deposit is linked to such keys, then one should have fewer hesitations in this respect.

Likewise, if restrictions are placed on the use of encryption keys of employees in the public administration only for communication related to the employees' work, then one should be no major misgivings about the requirements relating to back-up copies and possible deposit of such keys.

However, cases can be envisaged where routines for the use of a public administration employee's own key are based on the fact that the agency shall not unreservedly have access to information received by individual case officers. If such is the case, then stricter management routines will need to be considered than those which would otherwise apply to the agency's keys. Nevertheless,zero access to back-up copies or the deposit of encryption keys which are used for material relating to the activities of a public administration agency should only apply in exceptional cases.

Back-up copies and/or the deposit of encryption keys is conditional on having good routines for making back-up copies so that material does not become accessible by third parties. Access to such material should be accessed without time consuming routines when a need first arises. A request made by the head of the part of a public administration agency to which the encrypted material belongs, or the superior officer of the person concerned, should probably be adequate. Since the encrypted material, in accordance with the restrictions used here, relates to matters concerning the public administration agency in question, any further restrictions should not normally be necessary.

If individuals are also to be allowed general access to use their encryption keys for private purposes, the issue of back-up copies/deposit should probably be re-considered. However, it is recommended that the use of public administration agencies' and case officers' encryption keys should be reserved for material relating to the public administration agency concerned.

- Back-up copies of encryption keys which are used to decrypt messages sent to or sent internally within a public administration agency can be made, and several copies can be kept for security purposes.
- Back-up copies and the storage of encryption keys shall comply with recognised procedures relating to back-up copies and the storage of encryption keys.
- There should always be more than one copy of a key for decryption of material sent to or sent within a public administration agency.
- The agency's member of staff responsible for the archives (archive officer) should always have an extra key for the decryption of material sent to the agency.
- The archives officer can decide that copies of an encryption key used for decrypting material sent to a public administration agency should be deposited with another agency.
- Copies of keys used for decryption should be handed over at the request of the head of the public administration agency concerned, or that part of the agency to which the material, which has been encrypted using the encryption key in question, belongs.
- Requests for handing over keys should be made in writing. If an electronic request is submitted, it should be signed using the sender's digital signature or an alternative satisfactory technique designed to authenticate the origins of the message.

- Exceptions can be made from the rules applying to back-up copies or the deposit of encryption keys for special types of material. Such exceptions may be decided by the correct authority or be pursuant to a different regulatory framework (e.g. the protection instructions).

11.4 Stipulation of requirements and designation of satisfactory products and services

No requirements have been defined in respect of security products and services which the public administration agencies may wish to use. In cases where such agencies have joint standards, it would be a good idea to have a joint body which draws up requirements and evaluates these products and services.

- An agency should be appointed to draw up requirements relating to security products and services which are to be used by the public administration (at least if the ongoing standardisation work on the Directive on electronic signatures is not considered to be satisfactory, or if one wishes to use alternative security levels or services.)
- As far as "qualified certificates" are concerned, consideration needs to be given as to whether or not supplementary requirements should be stipulated. Any supplementary requirements would have to fall within the framework provided by Article 3(7) of Directive 1999/93/EC on electronic signatures, c.f. Section 5 of the draft Act relating to electronic signatures.
- A body should be appointed on behalf of the public administration to consider whether a given product/service meets such requirements.
- Requirements should be drawn up relating to documentation and any security reviews of suppliers of security services to public administration agencies.
- Requirements should be drawn up relating to cooperation with other suppliers of security services and products to the public administration.
- A public administration agency which opens its systems for electronic communication should ensure that products and services that meet the relevant requirements are available.
- The public administration agency should itself offer, or provide information about offers of, products and services which meet the relevant requirements.
- It shall always be assumed that the products/services offered via the public administration agency one is communicating with shall, in relation to individuals, always meet relevant requirements.

11.5 Legal means – guidelines, agreements, instructions or statutory regulations?

11.5.1 Guidelines

We envisage that the necessary guidelines for the use of digital signatures and encryption when communicating with and within the public administration could be provided in the form of instructions for users – a sort of "good practice" code which could be developed further by the so-called “market” through use.

Such "soft law" could probably be both appropriate and function well in many contexts. They could be particularly suitable in areas where industry or interested organisations are in a position to lay down guidelines for which a reasonable amount of support could be expected, or in areas where one can build on traditions and experience. In addition, "soft law" of this type will often serve as a supplement to more general, formulated statutory rights or obligations. They will probably, less often, represent basic principles in this area.

The regulations which this term of reference would like to be drawn up, and the area which they shall regulate, have other characteristics. First of all, we lack tradition and experience in large-scale electronic communication with the public administration. Secondly, we lack practical experience in respect of actual security services among "ordinary users." In addition, the public administration, probably via a coordinating body, do not constitute a strong influential force in relation to the variety of users at whom the regulations will be aimed.

Furthermore, the purpose of these regulations is to lay down the main rules on how electronic communication with the public administration can and should be carried out, with the opportunity for adapting solutions to the requirements of public administration agencies. Specific solutions, e.g. designing and operating certification services, monitoring and approval schemes, etc., can to a greater extent probably be developed "in the market." However, since these guidelines shall constitute the rules of action on which the public administration shall rely when their activities are to be opened up for electronic communication, we cannot risk that the regulations crumble away as a result of weaknesses in any self-regulatory mechanisms. Greater stability and predictability is required in the framework conditions if these are to form the basis of more comprehensive use of electronic communication.

11.5.2 Contractual regulation or statutory provisions

One alternative to mere recommendations and self-regulation may be that electronic communication between citizens and the public administration will be made dependent on there having been advance personal contacts and registration with the relevant public administration agency. If such is the case, we envisage that the necessary regulations for the use of electronic communication with the public administration are laid down in an agreement between the public administration agency concerned and the citizens.

The question may arise as to whether the authority exists to allow citizens to bind themselves in an agreement relating to how they should communicate with the public administration. Citizens can clearly not be deprived of their right to communicate orally or on paper in accordance with the Public Administration Act or special legislation in this respect. However, it is possible that contractual guidelines can be laid down relating to how they should proceed when they opt to make use of access to an alternative form of communication, such as electronic communication, which the public administration offers on its own initiative.

However, a model based on contractual regulation would easily become over-complex because different contractual practices could develop, and because it would be difficult to supervise the resultant practices with a view to coordinating measures. The problem is aggravated by the fact that this does not only involve the central public dministration. In addition, local administration and municipal administration should at least to a certain extent, operate under the same rules.

Contractual regulation in this context could also pose problems because it assumes contact between public administration agencies and individuals before security services can be used. This is probably acceptable as regards use by public administration employees in their work, or use by citizens of services which are administered by the public administration itself by, for example, giving user names and passwords/PIN codes in order to gain access to an information service. Nevertheless, prior contact between the parties is necessary in this context. However, as far as citizens are concerned, this will in many cases involve unnecessary extra work in having to enter into agreements with public administration agencies if messages are to be based on the use of, for example, qualified certificates issued by independent providers. In such a case, the public would normally enter into an agreement with the certification service provider. Furthermore, this would probably not be resolved by allowing certification service providers to look after the interests of the public authorities in this way. Such certification services would normally be used for several purposes, and it would be inexpedient, and probably impossible, to base public administration agencies' activities on allowing certification service providers to be responsible for entering into agreements with certificate holders with a content which particularly favours the needs of public administration agencies.

Another problem associated with using the contractual form as a tool, when seen from the point of view of the public administration, is that one cannot just simply make amendments those contracts which have been entered into. It is naturally important for individuals to have conditions of use which are as stable as possible. On the other hand, public administration needs to have uniform procedures which can be updated when dictated by developments. The rules which have been discussed in sections 11.2 and 11.3 about signature and encryption respectively also provide guidelines relating to the administration's opportunities for organising its own activities. It would not be acceptable if the opportunity to undertake reorganisation should be blocked because the public administration had entered into agreements relating to a specific method in respect of electronic communication. Rules should be an instrument for steering matters in the direction of efficient electronic communication, and not a straitjacket preventing sensible development.

Provided that suitable routines are established in respect of notifying users when conditions of use have been updated, the incorporation of regulations in a regulatory framework which can be updated, for example in accordance with the regulations relating to the provisions contained in the Public Administration Act, would be a more suitable tool than the use of agreements.

Naturally, this does not exclude the use of agreements as a means for making users especially attentive to those rules which do apply, and for emphasising to users, for example, the requirements for correct and proper use of signature and encryption keys, key-bearing cards and codes. However, the problems associated with the

implementation of the actual formation of contracts indicates that we should base ourselves on regulations which are incorporated in legislation.

11.5.3 Should internal public administration affairs be regulated by instructions?

The Committee assumes that the rules ought to be in a form which is more binding and more predictable for addressees than pure recommendations and codes of "good practice." We have also based ourselves on the fact that contractual regulation is not really the way to proceed, but that the rules can be laid down in a regulation. A regulation of this type can obviously be rooted in the Public Administration Act and if necessary in the Act relating to electronic signatures.

The question is whether or not the guidelines touch on internal public administration circumstances which might be more suitable to regulate through instructions. This could provide greater flexibility when developing and adapting the regulatory framework. In addition, one would avoid regulations directed at the general public from being more comprehensive than necessary.

On the other hand extra challenges would be created in respect of administering and maintaining the regulatory framework because there is a close inner connection between rules which are directed at the internal functions of the public administration and the regulation of citizens' rights and obligations in respect of communicating with the public administration. There is also a problem associated with the fact that since municipal authorities are also to be included, the briefing authority for a central administrative agency would not necessarily be adequate, and it appears to be unnatural to introduce a special briefing authority in this area. It would appear to be better to operate with regulations based in legislation in respect of those rules which are to be common for all public administration agencies in both central and local administration.

Nevertheless, some matters can or should be resolved through instructions. This applies, for example, to the provisions relating to who signs what and who is entitled to approve the issue of certificates to public administration employees, etc. Citizens' rights in accordance with such certificates can be linked to objective characteristics on the issued certificates without citizens needing to concern themselves about the extent to which the underlying routines have been followed, c.f. the proposals relating the use of "seals" in point 11.2.5.

Similar assessments could probably be made as regards systems and security services which have been organised or appointed by the public administration. It should not be the citizens' problem if there has been a breach of internal instructions, provided that the outward systems appear as having been "approved."

The appointment or organisation of an agency which is to draw up requirements relating to security services for the public administration and for the evaluation or approval based on external assessment reports of such services and products can be carried out through a set of instructions. The same applies to the guidelines which

have been laid down for the procurement of such services by each public administration agency. Obviously this shall apply within the framework of the rules relating to public procurement and those considerations which apply to the particular area of public administration when switching over to electronic communication, such as the considerations which lie behind legislative requirements relating to form, c.f. for example the report on the Kartleggingsprosjekt (the Mapping Project) [47].

The rules should be uniform. If the rules and responsibility for such are split between regulations and instructions and between different administrative levels, problems arise which would need to resolved by, for example, having good routines for the administration and maintenance of the regulatory framework which would ensure that the connection between internal and external regulatory frameworks and between different administrators of regulatory frameworks would be taken care of.

11.5.4 Summary of tools

It is thus recommended that, as far as possible, necessary rules should be laid down in the regulations which are based on the Public Administration Act and, if necessary, the Act relating to electronic signatures.

Internal public administration matters relating to the drawing up of requirements, approving and obtaining security services and products for the public administration, as well as rules relating to internal case processing, can be resolved, for example, through instructions.

The legal effects of the fact that one has used systems that have been selected or approved by the public administration, or certificates belonging to the public administrtion, must be apparent in the regulations or the legislation on which they are based.

11.6 Draft regulations on electronic communication with and within the public administration

11.6.1 Signature and authentication

Addressees for enquires to the public administration

1. Electronic communication sent to a public administration agency should be directed to the address stipulated by the relevant public administration agency for these sorts of enquiries.
2. If a public administration agency has set up its system for enquiries, or certain types of enquiries, via a separate website/homepage, electronic communication should be sent/received in the manner arranged.
3. Electronic enquiries relating to a public administration agency and sent directly to a case officer shall only occur if the public administration agency has set up its system for such and has expressly permitted this sort of direct communication either in general or in particular cases.

4. Public administration agencies may reject messages which have been sent in a different form or to a different address or in a different way to that prescribed or set up. Public administration agencies shall at the same time provide notification of the correct address, form or procedure. Such information may be provided in the form of a reference to or the circulation of guidelines about the situation.
5. Public administration agencies may decide that messages for public administration agencies should be addressed direct to a case officer only when such messages are sent from another public administration agency.

Messages which activate an obligation to provide guidance – form-free messages

1. Enquiries sent to public administration agencies which are not subject to special form requirements, and which do not activate case processing, can be sent electronically without using security services.
2. In certain cases, public administration agencies can request information to confirm the identity or authority of the sender if this is important for the handling of the enquiry concerned.

Applications and other enquiries which actuate case processing (related to a specific case)

1. Enquiries which activate case processing, but which are not subject to special form requirements, can be sent without using security services.
2. In certain cases, the public administration agency can request information to confirm the identity or authority of the sender if this is important for the handling of the enquiry concerned. The public administration agency can also request that special security services should be used.
3. The public administration agency can determine that such requirements shall apply in general to enquiries which have been specified in greater detail.
4. The public administration agency shall offer, or provide instructions about, services which enable compliance with requirements for confirming identity or authority or other requirements stipulated by the public administration agency.

Messages subject to form requirements

1. For enquiries which are subject to special form requirements, the public administration agency can provide instructions about which tools need to be used so that these kinds of enquiries can be sent electronically, including requirements relating to tools for the secure confirmation of the sender's identity or authority. The public administration agency can also request that special security services be used.
2. The public administration agency shall offer, or provide instructions about, services which enable compliance with the requirement for confirming identity or authority or other requirements stipulated by the public administration agency.

Messages which do not meet relevant requirements

1. A public administration agency which receives enquiries in electronic form which do not meet relevant requirements for such messages, shall inform the sender about such without undue delay, and advise which measures need to be implemented so that the enquiry in question can be accepted for processing.
2. Such guidance can be provided by referring to the public administration agency's published rules relating to the handling of the type of message in question.

3. The public administration agency shall record the time when such an enquiry is sent, and to whom.
4. If an error is such that it is not possible to identify the sender, and notification cannot be sent, information to this effect shall be recorded.
5. The general rules relating to rejection and redress contained in the Public Administration Act shall apply to the circumstances mentioned.

Notification about decisions

1. Notification about individual decisions can take place electronically if the person to whom the decision applies/who is entitled to such notification, has consented to such.
2. Notification about decisions shall be accessible from an information system which is suitable for this purpose.
3. The person to whom a decision applies shall receive notification to the effect that the said decision has been adopted, and about where and how the person concerned can obtain knowledge about the contents, as well as a deadline for when such can be obtained.
4. The contents of a decision shall be made available to the party concerned once they have confirmed their connection with the matter to the information system on which the decision has been placed (authentication).
5. The information system shall record the time when the party concerned obtained access to the decision, as well as data which confirms the party's connection with the case.
6. Notification is considered to have occurred at the time when the party concerned obtained access to the decision.
7. If the party concerned has failed to obtain access to the decision within 7 days of the date on which notification of the decision was sent, or made available, notification to this effect shall take place in accordance with those rules which apply to the notification of individual decisions relating to the area concerned when consent has not been given for electronic communication.

Complaints

1. Complaints about individual decisions can be sent electronically if the public administration agency concerned has set up its system for this, or if notification about a decision has been made electronically.
2. The public administration agency can request information to confirm the identity or authority of the sender if such is necessary for dealing with the complaint. The administrative agency can also request that special security services should be used.
3. The public administration agency shall offer, or provide instructions about, services which enable compliance with requirements for confirming identity or authority or other requirements stipulated by the public administration agency.
4. If a complaint is submitted electronically, and the public administration agency concerned has set up its system for complaints via its information system, this procedure shall be used.
5. A public administration agency which receivey complaints in electronic form shall immediately send a receipt to the sender in respect of the complaint received.
6. Complainants have the duty to check to ensure that they have received a receipt for complaints they have submitted. If a receipt has not been received within 24

hours, the complainant shall re-submit his/her complaint, specifying when it was sent the first time.

Access to information and documents in electronic form

1. Requests for access to documents or information relating to a case can be submitted electronically to the public administration agency.
2. In certain cases, the public administration agency can request information to confirm the identity or authority of the sender if this is important for the handling of the message concerned. The public administration agency can also request that special security services should be used.
3. If a public administration agency has electronic archives, access can be provided electronically.
4. Unless access can be demanded in accordance with the Freedom of Information Act, electronic access shall only be provided on condition that satisfactory confirmation can be provided of the party's connection to the case concerned, and that assurance can be provided that the documents are only made available to the party concerned.

Hearings and comments for the hearing regarding regulations, etc.

1. Discussion documents (for the hearing) sent to addressees with their own or a central e-mail reception facility can be sent electronically. Instead of sending a covering letter complete with discussion documents, a message can be sent about where the discussion document is available for viewing along with an invitation to obtain access within a specified time. If the person concerned has not gained access to the discussion document within the specified deadline, the discussion document should be sent in paper-based form, unless the public administration agency concerned has decided otherwise in respect of the consultation concerned.
2. Comments on the hearing documents may be submitted electronically. Such statements shall be sent to the e-mail address specified by the public administration agency concerned for the relevant consultation, or in a different way as instructed by that agency.
3. The public administration agency can request information to confirm the identity or authority of the sender if this is important for the handling of the comments concerned. The public administration agency can also request that special security services should be used.
4. The public administration agency shall offer, or provide instructions about, services which make it possible to comply with requirements relating to the confirmation of identity or authority or other requirements stipulated by the pubic administration agency.

Archives and long-term storage

1. A message which hay been signed with a digital signature, and which is to be filed, shall be filed with the certificate which confirms the signature and other information necessary for verifying the signature, including confirmation that the certificate had not been revoked at the time verification occurred.
2. As regards messages where a certificate's period of validity is shorter than the time it may take to confirm the contents of the message, and messages which when filed or during their period of storage are converted into a different format, the archives shall verify the signature upon receipt, and then suitably confirm the connection between the message, the message's signature and the actual

certificate along with information about the time such confirmation took place. The archives shall secure the integrity of the messages and the confirmation of the mentioned conditions during the period of storage. The archives can decide that this procedure should also be used for other messages (than those mentioned in the first sentence).

3. If the archives fail to verify the signature, information to this effect shall be stored, if possible with information on the reason why such verification failed.
4. Messages or the results of automated data processing (e.g. from automated services with web interfaces) which have been confirmed using other authentication techniques than digital signatures, shall be stored with information to the effect that correct authentication has taken place, and, if possible, which techniques have been used.

11.6.2 Content encryption and key handling

Issue and use of certificates for information systems

1. Information systems which are used in connection with either fully or partially automated processing, and which in their results are or emerge as decisions in accordance with the Public Administration Act, shall be equipped with a certificate which identify the agency for which the information system concerned processes messages.
2. The certificate shall contain information which provides the recipient of the certificate with confirmation of the connection between the processing carried out by the information system and the agency concerned.
3. Recipients of messages relating to such certificates can relate to the message as though it had been signed by an employee of a public administration agency with the authority to submit or sign such messages or decisions, unless the person concerned knew, or should have known, that the message or decision concerned had occurred as the result of an error.
4. Applications for the issue of certificates which link signature-verification data (public keys) to an information system and a public agency, and which are to be used for processing which can result in decisions made in accordance with the Public Administration Act, shall be approved by the person who has been authorised to grant authority on behalf of the agency concerned.

Observations re. vulnerability – securing keys for information systems

1. For an information system which is equipped with certificates for public administration agency, routines shall be drawn up which ensure that the system concerned can be put into operation rapidly with new signature-creation data and a new certificate if the certificate which is being used is revoked or if signature-creation data is lost.
2. It should be considered whether or not the information system should be equipped with signature-creation data and certificates from more than one certification service provider.
3. Signature-creation data should be secured against misuse in accordance with recognised principles relating to information system security.

Procurement of keys, codes and certificates

1. A public administration agency can provide its employees with instructions about which security services they should use when carrying out their duties, and where they should apply or how they should proceed to obtain necessary keys, codes, certificates, etc.
2. While carrying out their duties for their employer, public administration employees should only use certificates issued by certification service providers who have been approved by their employer or by a public administration agency which is responsible for coordinating that agency's activities.
3. Coordinating public administration agencies can decide that when work is being carried out for public administration agencies, use can only be made of certificates issued by certification services providers who have entered into a framework agreement for the supply of such services to the agency.
4. If a framework agreement expires and is not renewed during the course of a certificate's period of validity, the certificate can nevertheless be used for the remainder of the period of validity, unless the certification service provider's certificate is revoked, or the necessary catalogue services, etc. are no longer available.
5. Coordinating public administration agencies can decide that such certificates shall nevertheless not be used once a framework agreement has expired.

Collection of information and consent re. handing over of certificates, etc.

1. The collection of information which is to be used in a certificate shall be obtained directly from the person to whom the information applies, or with his/her express consent, cf. Section 7 of the Act relating to electronic signatures [52].
2. The certification service providers shall request the employee's consent for the delivery of the certificate to others, in connection with applications from public administration employees for certificates for use in service, cf. (presumably) sub-paragraph (b) of the second paragraph of Section 14 of the Act relating to electronic signatures.
3. One should seek consent for handing over information about an employee's duties or authority in service when this information is stored in linked catalogues and not directly in the actual certificate, provided that this information can be expected to have a bearing on the use of the certificate. Such information may only be handed over in connection with verification of the relevant certificate.

Guidance for employees

1. When obtaining keys, codes and certificates, employees shall receive information/guidance about:
2. Responsibilities and obligations regarding the storage and use of keys, codes and certificates, etc.,
3. Current certificate policy and practice (in the form of an adapted user version),
4. Their own and others' possibility to blacklist or suspend certificates,
5. Expiry of certificates,
6. Certification service providers' storage of personal information, storage periods and to whom certificates can be issued, etc., cf. Section 19 of the Personal Data Act,
7. Responsibilities and obligations of certification service providers,
8. Responsibilities and obligations of the registration authority,
9. Restrictions on the use of certificates.

Restrictions on the use of keys, codes and certificates

1. Authentication data or certificates (e.g. employee certificates) which contain pointers to a public administration agency in its capacity as an employer shall only be used when carrying out duties for the employer in question.
2. Personal (private) certificates shall not be used when carrying out duties for an employer.

Requirements concerning the proper use and storage of employee keys/key-bearing media

1. Owners of signature-creation data shall store and use it such that it does not become accessible to others.
2. Signature-creation data shall only be used for the purposes for which it is issued.
3. The owner shall never leave his/her workstation, terminal or other unit used for authentication or signature generation without ensuring that signature-creation data is no longer accessible on/in the unit, that the current session has been terminated, or that the unit has otherwise been secured against misuse.
4. The owner of signature-creation data shall not hand it over to others or give others access to it, not even when others are going to act on his/her behalf. If someone is going to act on behalf of another party (with authority), this shall occur with the authorised representative's own signature-creation data with mention of the fact that the message has been delivered on behalf of someone else. (The person for whom someone acts on behalf of can issue a role certificate to his authorised representative (when this becomes available)).
5. The provisions on signature-creation data apply likewise to the use of authentication data (passwords/PIN codes).
6. Employees shall otherwise follow the instructions laid down by their employer relating to the use and security of the enterprise's information system, including information about checks on material which is to be downloaded or installed in the information system.

Notification obligationsupon loss of keys, suspicion of misuse, etc.

1. The owner of signature-creation data or authentication data should immediately notify the certification service provider or the person who has been appointed to receive such notification if there is suspicion that signature-creation data or authentication data are lost, gone astray, or are otherwise being, or could be, misused.

Requirements relating to the control of certificates and revocation lists

1. If a message which is equipped with an electronic signature cannot be verified in accordance with the rules which apply to the type of message in question, and if this is important for processing of the message in the public administration agency, a message should be sent to the sender in accordance with the rules mentioned under point 11.2.3.

Requirements/recommendations re. local storage of certificates, etc.

1. Copies of relevant certificate(s) and other information necessary for the verification of signatures over time should be stored in the archives.
2. If a message, for a period of time, is stored locally by the user, without being sent to the archives, information to this effect should be stored locally along with the message.

Choice of security service

1. When engaging in electronic communication with public administration agencies, individuals must use services which comply with the stipulated requirements for the application in question.
2. If qualified signatures are used, individuals may themselves select which supplier of qualified certificates they wish to use.
3. The public administration may stipulate additional requirements within the framework of Section 5 of the Act relating to electronic signatures.

Guidance for users

1. When obtaining keys, codes and certificates, users should receive information/guidance about:
   Responsibilities and obligations regarding the storage and use of keys, codes and certificates, etc.
2. Current certificate policy and practice (in the form of an adapted user version),
3. Their own and others' possibilities to blacklist or suspend the certificate,
4. Expiry of the certificate,
5. Certification service providers' storage of personal information, storage periods and to whom certificates can be issued, etc., cf. Section 19 of the Personal Data Act,
6. Responsibilities and obligations of the certification service provider,
7. Responsibilities and obligations of the registration authority
8. Restrictions on the use of the certificate.

Restrictions on the use of keys, codes and certificates

1. Signature-creation data or authentication data which are assigned to individuals particularly for communication with the public administration should not be used for other purposes.
2. Such restrictions should appear on the certificate and the user should be informed about them, cf. the above guidelines.

Requirements for the proper use and storage of keys/key-bearing media

1. The owner of signature-creation data shall store and use it so that it does not become accessible to others.
2. Signature-creation data shall only be used for the purposes for which it is issued.
3. The owner of signature-creation data should never leave his/her workstation, terminal or other unit used for authentication or signature generation without ensuring that the signature-creation data is no longer available on/in the unit, that the current session has been terminated, or that the unit has otherwise been secured against misuse.
4. The owner of signature-creation data shall not entrust it to others or give others with access to it, not even to others who are going to act on his/her behalf. If someone is going to act on behalf of another party (with authority), this shall occur with the authorised representative's own signature-creation data with a reference to the fact that the message has been delivered on behalf of someone else. (The person for whom someone acts on behalf of can issue a role certificate to his authorised representative (when this becomes available)).
5. The provisions relating to signature-creation data apply likewise to the use of authentication data (passwords/PIN codes).

6. The owner of signature-creation data should only use these in information systems in which he/she have confidence, and follow the recommendations provided by the certification service provider about adjusting and using the system. Caution should be displayed if changes are made to the system, and one should check material which is to be downloaded or installed in the information system.

Notification obligations upon loss of keys, suspicion of misuse, etc.

1. The owner of signature-creation data or authentication data should immediately notify the certification service provider or the person who has been appointed to receive such notification, if it is suspected that signature-creation data or authentication data are lost, have gone astray, or are otherwise being, or could be, misused.

Requirements relating to the control of certificates and revocation lists

1. If a message which is equipped with an electronic signature cannot be verified in accordance with the regulations which apply to the type of message in question, and if this has a bearing on the processing of the message, a message should be sent to the sender.

Requirements for/recommendations on local storage of certificates, etc.

1. Storage of relevant certificate(s) and other information necessary for the verification of signatures used when communicating with a public administration agency is something which individuals can entrust to the public administration agency's archives.
2. The manner in which long-term storage and hand over to individuals will occur is subject to the rules which apply to the archives at any one time.
3. During the period when the actual transaction or the exchange of information takes place, individuals should also store necessary information locally themselves.

Intervention re. misuse of certificates when communicating with the public administration

1. In the event of well founded suspicion relating to the misuse of a certificate when communicating with a public administration agency, the agency concerned can deny access by blacklisting the user's identity or the certificate to prevent further use against the agency. The same applies if a certificate owner misuses his permission or access to communicate electronically with the agency concerned.
2. Before a certificate is blacklisted, the public administration agency concerned shall notify the certificate holder that they are considering blacklisting the certificate, and state their reasons for doing so. The certificate holder should be encouraged to comment on the reason for the blacklisting. The public administration agency shall set a deadline for such statements (which shall not be less than (number) days).
3. If, after having considered the certificate holder's comments, the public administration agency decides to blacklist the certificate, it should forward notice to this effect immediately to the certificate holder.
4. The certificate holder can appeal against a decision to blacklist.
5. Appeals against the blacklisting of certificates should be processed as rapidly as possible, and the appeal body can decide that an appeal shall be postponed.

6. The administrative appeal body dealing with the blacklisting of a certificate shall be appointed by the King/coordinating ministries. Special regulations may be laid down relating to the processing of appeals against the certificates.
7. Such provisions shall apply similarly to the blacklisting of authentication data (user name and accompanying password/PIN code) in information systems set up by a public administration agency where such are suitable.

Copying signature keys

1. Signature keys issued to individuals shall not be copied.

Information for citizens when sending personal data and confidential information to the public administration

2. A public administration agency which sets up its system for receiving information from individuals or organisations, which it may be required to keep confidential or which is subject to security requirements in accordance with the regulations relating to the processing of personal data, shall inform the individual concerned in a suitable manner about any risks involved in the electronic transmission of the information concerned.
3. The public administration agency shall make necessary security services readily available to individuals, or provide information which makes it easy for individuals to gain access to such services.
4. The public administration agency shall also (on request) provide information about how personal data or confidential information are secured while such data is being processed by the agency concerned.
5. If the risk of unauthorised access to confidential information or personal data cannot be prevented in a simple manner by the individual concerned, the public administration agency shall not set up its own system for this kind of communication.

Encryption of messages sent to the public administration

1. When encrypting a message sent to the public administration, an encryption key linked to the public administration agency concerned should be used.
2. Encryption using an encryption key linked to a case officer can only be undertaken if the agency concerned has its system set up for this.

Receipt of encrypted material

1. Messages received by public administration agencies in encrypted form shall be decrypted immediately.
2. If it is not possible to decrypt a message upon receipt, the message should be returned to the sender immediately with a message stating that it was not possible to decrypt the message (not accessible by the public administration agency or other recipient), and that a new message must be sent.
3. A message returned on this basis should be recorded/logged by the public administration agency along with information about who the sender was, the time when the message was received and returned, and a description of the contents of the message, if known (e.g. through an open title, etc.).
4. For a message which is returned because it is not accessible by the public administration agency concerned because a different encryption key has been used than the one specified by the agency (or because the contents of the message are not accessible to the public administration agency for other reasons), the

provisions contained in the Public Administration Act relating to rejection and redress shall apply.
5. The protection of data in an agency's own internal system is carried out using the tools which the agency or coordinating body concerned has decided are necessary and suitable.

Deposit or other back-up copies of encryption keys
1. Encryption keys, which are used to decrypt messages sent to or sent internally within a public administration agency, can be backed up, and several copies can be kept for security purposes.
2. Such back-up copies and the storage of encryption keys shall comply with recognised procedures relating to back-up copies and the storage of encryption keys.
3. There should always be more than one copy of a decryption key for material sent to or sent within a public administration agency.
4. The agency's member of staff responsible for the archives (archive officer) should always have an extra key for the decryption of material sent to the agency.
5. The archive officer can decide that copies of an encryption key used for decrypting material sent to a public administration agency should be deposited with a different agency.
6. Copies of keys used for decryption should be handed over at the request of the manager of the public administration agency concerned, or that part of the agency to which the material, which has been encrypted using the encryption key in question, belongs.
7. Such requests should be made in writing. If a request is submitted electronically, it should be signed using the sender's digital signature or a different satisfactory technique designed to authenticate the origins of the message.
8. Exceptions can be made from the rules which apply to back-up copies or the deposit of encryption keys for special types of material. Such exceptions may be decided by the correct authority or be pursuant to a different regulatory framework (e.g. the protection instructions).

11.6.3 Stipulation of requirements and designation of satisfactory solutions

Stipulation of requirements and designation of satisfactory solutions
1. An agency should be appointed to draw up requirements relating to security products and services which are to be used by public administration agencies (at least if the ongoing standardisation work on the Directive on electronic signatures is considered unsatisfactory, or if one wishes to use alternative security levels or services.)
2. As far as "qualified certificates" are concerned, consideration needs to be given to whether or not supplementary requirements should be stipulated. Any supplementary requirements would have to fall within the framework provided by Article 3(7) of Directive 1999/93/EC on electronic signatures, c.f. Section 5 of the draft Act on electronic signatures.
3. An agency should be appointed to consider on behalf of the public administration whether a given product/service meets such requirements.

4. Requirements should be drawn up relating to documentation and any security reviews of suppliers of security services provided to public administration agencies.
5. Requirements should be drawn up relating to co-operation with other suppliers of security services and products to the public administration.
6. A public administration agency which sets up its own systems for electronic communication should ensure that products and services are available which meet the relevant requirements.
7. The public administration agency should itself offer, or provide information about, offers of products and services which meet the relevant requirements.
8. Products/services, which are offered via the public administration agency with which communication takes place, shall always be considered to meet relevant requirements relating to the individual products/services concerned.

11.7 Proposals for further actions

The Committee recommends that a review be carried out to find out which internal routines and programmes need to be established in respect of linking up to mail reception facilities and archives before commencing with digital signatures and content encryption.

- It should be considered whether or not the Public Administration Act should allow for fully automated decision-making processes, and the types of vulnerability which this would open up for.
- The Committee recommends that consideration should be given to other ways of regulating the requirements contained in the protection instructions than those which are currently provided for in the current instructions. One solution could be to consider whether or not these rules, either fully or partially, can be incorporated in possible new regulations under the Public Administration Act, e.g. as supplementary rules relating to the Act's enjoinder to treat confidential information in a satisfactory manner. Consideration should be given *i.a.* to whether it might be possible to coordinate requirements relating to the classification of "Confidential" in the protection instructions with requirements relating to, for example, confidentiality and the securing of sensitive personal data. The Committee therefore believes that the protection instructions should be abolished, provided that suitable alternatives exist which the public administration will be better served with.
- If the protection instructions are retained in their present form, the Committee believes that it is important to reassess which rules should apply to information which has been classified in accordance with the protection instructions when engaging in electronic messages. The Committee believes that it should be possible to deal with electronic processing of information which has been classified as "Confidential" in accordance with the regulations which are proposed in this report, with a necessary amplification of standards and recommended security levels. The Committee thus believes that rules relating to the electronic processing of information which has been classified as "Confidential" could build on or be coordinated with the Committee's draft regulatory framework.

- Consideration should be given to whether special regulations should be drawn up in respect of interruption of deadlines when complaints are submitted electronically, e.g. when a complaint is sent over a dedicated information service set up by a public administration agency.
- Consideration should be given to solutions based on the fact that a public administration agency should always acknowledge receipt for complaints which have been received.
- Consideration should also be given to whether messages which are neither case documents (this can, if necessary, be linked to whether they should be recorded and/or filed under the Archives Act) nor relevant as documentation under financial regulations, should be completely exempt from the rules relating to the use of authentication services or signature technology.
- A review should also be carried out into the need for, and any requirements relating to, the use of time stamping and storage of information by a trusted third party, if the public administration and the people have such need.
- Consideration should be given to whether overall functional requirements should be placed on storage which will be met by *i.a.* standards such as Noark-4 [57] (the approved standard for electronic filing systems in accordance with the Archives Act and its appurtenant regulations), and the European standard for (extended) signature formats (ETSI ES 201 733).

13 Qualitative, administrative and financial consequences

13.1 Principles

In order to achieve the political aim of renewing the public sector, including the introduction of 24/7 government administration, the Committee feels that solutions which ensure a secure, efficient and reliable infrastructure for the electronic exchange of information are important instruments. The Committee therefore proposes certain central, joint measures. In addition, the Committee proposes a series of voluntary measures, which the individual department or unit must in principle take on its own account.

The central actions proposed by the Committee are in outline as follows:

- Establishing a coordination function consisting of a new, permanent coordination committee for the common needs of the Government administration, led by the Ministry of Labour and Government Administration or the Ministry of Trade and Industry, with a secretariat,
- Establishing a Forum for Digital Signatures for the Government, industry and suppliers,
- Establishing a new framework agreement for Government,
- Entering into contracts with players in the market for the issue of certificates to individuals,
- Using incentives to promote the use of digital signatures in electronic interaction with and within the Government administration.

The Committee's proposals are designed primarily to aid development of the whole environment for secure electronic administration and communication, regardless of the time of day or geography. This will give improved and more efficient access to secure electronic services from the public sector, both for individuals and industry, and will increase productivity within the Government administration itself. It is important that as many people as possible take part in this development, so that the solutions are not only useful for those with the most resources. The implementation of these actions will involve certain initial and running costs for the administration. In the opinion of the Committee, it is both necessary and natural for the administration to cover these costs on behalf of the community.

The Committee considers it essential that the necessary costs entailed in establishing *important joint solutions* are covered centrally by the State, but that the individual organisation should otherwise cover the costs of using digital signatures and encryption from its own budget, within the time limits the Government has laid down in order to achieve the aims of 24/7 and electronic government services by the year 2003.

The Committee's proposals would promote *qualitative utility* of the systems for individual government agencies, the government in general, individual persons and industry (see Point 13.2). The Committee believes that it would be virtually

impossible to offer certain services electronically without using digital signatures, or that even if it were possible, they would be less secure and/or of poorer quality. The *administrative* consequences of the report's recommendations are closely related to new or changed functions and areas of responsibility, both within the individual administrative agencies and collectively for all or parts of the Government administration (see Point 13.3). The *financial* consequences present a far more complex picture. The Committee has not been able to explore these in detail. In a number of areas, one can only hint at the direction developments might take, while in other cases, one can quantify financial aspects (see Point 13.4).

13.2 Qualitative considerations

13.2.1 Cost/benefit analysis for the use of PKI (Public Key Infrastructure) technology

The usefulness of electronic case processing and electronic services is related both to the financial savings for the Government administration itself and for those they communicate with, and to the improved quality of public services. Qualitative improvements are primarily related to faster case processing and improved access, regardless of location or opening hours. In many cases, however, electronic services will also reduce the risk of error, in the data on which a decision in a case is based, for example.

It is important to be aware of the fact that digital signatures and PKI are only valuable to the extent that they are applied for specific purposes. Moreover, digital signatures are not only a security measure, but a technology that makes new electronic services possible. The discussion under Points 13.4.2 and 13.4.4 gives a reason for this point of view.

Electronic services and electronic case processing in the public sector will make different demands depending on the type of service or case processing. A central question, which must be considered in each particular case, is the need for digital signatures and encryption of messages in connection with electronic documents.

Where there is no need for a signature, it may nevertheless be desirable to use PKI to provide secure identification for, and authentication of, users when using a public electronic service, for example. The technology may also, through encryption, protect a message against prying and unauthorised alteration, in certain cases.

An example of improved quality related to the use of PKI is the Directorate of Taxes' service of pre-completed tax assessment forms. Until now, one has here used a PIN-code based authentication, and with this level of security one can offer a certain range of information and operations. The next step, operational as a pilot version in the spring of 2001, is authentication based on PKI, but not on digital signatures. This gives increased security and the possibility of more personalised services and a wider range of functions and information. The following version will also bring digital

signatures into use and it will then be possible to offer a full electronic tax assessment service.

The introduction of electronic services must follow cost/benefit analyses and risk assessments in which the costs and benefits of using PKI will often be central. At present, this technology is viewed as complex, which also means that the costs can be high. But, as mentioned above, the usefulness may in certain cases be such that services cannot be offered electronically without the use of this technology – when a signature is needed, for example. One must then weigh up what is gained by offering the services electronically.

It is also clear that if an infrastructure with its users already exists, new services can be based on this which will have quite different cost/benefit analyses from those one would make initially for the first versions of services based on digital signatures.

One should consider:
- Increased costs against other possibilities that may yield greater benefits – access to alternative methods, for example, and the costs relating to these.
- Increased costs involved in maintaining two parallel systems, one paper-based and the other electronic. This includes the maintenance of skills related to manual routines that one may not need in connection with an electronic system.
- Whether electronic transactions can incur costs for the other party. High costs may limit the number of possible users, which in turn limits the benefit of electronic communication.
- The development and maintenance costs of electronic communication.
- Whether it is possible to change the underlying routines associated with manual case processing so that these can be automated.
- How the theoretical gains in efficiency on changing to electronic services can be realised in practice.
- Requirements for signatures under existing law.
- Customary and established practice within the sector concerned.

13.2.2 Risk assessment as a factor in cost/benefit analysis

It is essential in a cost/benefit analysis to consider the risk of loss or damage which may arise with the use, or non-use, of PKI.

Risk assessment must be undertaken where the information is considered sensitive in some way, for individuals or companies, for case processing and decision-making, or for the agency as such. The assessment must identify techniques and management procedures that optimally minimise risks, have acceptable costs and maximise benefits for the parties concerned. Much can be quantified, but some factors can only be estimated qualitatively. It may, for example, be difficult to assess the value of measures to prevent fraud.

In the course of cost/benefit analysis one looks at:
- The probability of damage or loss arising,
- The costs of potential damage,

– The costs of taking preventive security measures and actions for making good any damage, and the costs of doing nothing.

The alternatives that establish an acceptable level of risk should be expressed as the net benefit for both the Government administration and for individuals or companies. If the benefit is negative, the Government may conclude that for the time being it would not be natural to introduce electronic communication in the area concerned.

On the other hand, it is not the case that all cost/benefit analyses are decided by a risk assessment. An action may well have negative (or positive) benefits even if there is no risk. Net benefit is decided by whether the costs are greater or less than the calculated benefits.

A risk assessment will always have to be linked to considerations relating to relevant laws and regulations (regarding protection of privacy, for example) so that the level of security is high enough to satisfy the statutory requirements.

13.3 Administrative consequences

13.3.1 Shared administrative consequences

Established arrangements

Certain joint administrative functions have already been set up:
– The Norwegian Post and Telecommunications Authority has, under the new law and regulations on electronic signatures, been given responsibility for supervising certification service providers that issue approved signatures [52].
– *Norsk Akkreditering* (Norwegian Accreditation) has been commissioned by the Ministry of Trade and Industry to set up a Norwegian system for the accreditation and certification of information security within organisations (cf. Govt. White Paper No. 1 (1989-99), Ministry of Trade and Industry). The certification system and British Standard BS 7799 are described in detail by Norsk Akkreditering. See Internet: http://www.justervesenet.no/na/default.htm. Select "informasjonssikkerhet." The system can to some extent help to create a basis for confidence in the general security of information, for example with the certification service providers, but not for security specifically related to digital signatures, etc.
– The *Storting* (Norwegian parliament) approved the Government's proposal (White Paper No. 1 (1989-99), Ministry of Trade and Industry) and gave FO/S (HQ Defence Command Norway/Security Control) authority to certify and/or approve the IT security of products and systems. The scheme is intended for the civilian sector and is based on voluntary participation. Whether FO/S will have any duties relating to the approval of secure electronic signature creation systems has not yet been clarified.
– The Norwegian Technology Centre has responsibility for making and issuing standards for the areas concerned. Work is now (January 2001) in progress on the

translation into Norwegian of a new international standard (IS 17799) for the security of information within organisations, based on the above-mentioned British Standard BS 7799, Part I.

– A purchasing scheme for certificates, software for digital signatures and the encryption of messages, smart cards and smart card readers, has been set up under the auspices of *Forvaltningsnettsamarbeidet* (The Public Administration Network Cooperation, or FNS). All administrative departments can use these framework agreements when purchasing.

Proposed arrangements

This report concludes that there is a need to place the responsibility for coordinating government work in the field of digital signatures and PKI with a single body. The Committee proposes the establishment of a coordinating function in the form of a permanent coordinating committee with a secretariat, cf. Point 9.6. This would be a new function within the Government administration. The location of the secretariat must be decided.

The coordinating function will have the overall responsibility for setting quality and security requirements for solutions within the Government and for the boundary between the public and the private sector (both organisations and individuals). It will have responsibility for the Government's joint specifications in collaboration with those responsible for procurement and framework agreements, as for example with the Public Administration Network Cooperation and with the supervisory authorities and standardisation agencies.

This report also concludes that a common *Forum for Digital Signatures* for the Government administration, industry and suppliers of certification services, ought to be set up. Issues relating to coordinated traffic services will be particularly important for such a forum.

Joint projects, applications, services, etc.

In addition to projects within individual government agencies, there are many examples of collaborative projects involving several administrative units, among them the health sector (led by the National Insurance Administration, for example), information exchange projects (Directorate of Taxes, Statistics Norway and the Brønnøysund registers) and others. More such collaborative projects should be encouraged.

A potential for cooperation on common services has been identified. In the field of digital signatures and PKI this applies particularly to coordinated traffic services for the verification of certificates. This report recommends work on coordinated traffic services, but does not recommend starting new work on certificate directories now.

The Public Procurement Department of Government services is working on the establishment of an electronic marketplace for the Government administration. There is a clear need for electronic signatures in such matters and it is important to have a coordinating body involved in this and similar projects, in connection with the Ministry of Trade and Industry’s work on e-commerce, for example.

Building skills

IT infrastructures can be large and complex. In order to understand them it is useful to see them as a whole and to understand how they relate to each other [31]. The most important skill is probably not related only to technology but to the relationship between technology and institutional and social structures in the community. PKI is a sub-field that is both complex and new. Great changes happen quickly. The proposed coordinating body must not only have a role and have good knowledge within the field: efficient exploitation of PKI also demands knowledge of the individual government agencies. Setting up training courses and other skill-developing measures will be of great significance in the PKI field. It will be natural for *Statskonsult* (the Directorate of Public Management) as the Government's central body for skill development and training to get involved in this and to build up the service in line with further needs in the field.

A number of government agencies have excellent skills. The challenges lie rather in getting the people concerned to work together as much as possible, both in terms of concrete tasks and to build up and exchange skills. The proposed coordinating body may be given special responsibility for maintaining an overview of relevant skills environments and individuals and for stimulating professional contact.

Shared administrative consequences will also be linked to contact with research and development partners, and to contact with suppliers of products and services. There will also be international standardisation work that must be pursued, including making and maintaining contacts with relevant international partners. This is a job that must be undertaken by the relevant standardisation organisations such as the Norwegian Technology Centre and Statskonsult's secretariat for IT standardisation in government administration, and which may require additional resources.

13.3.2 Administrative consequences for government agencies

Establishment of digital signatures and certificates

If the government agency itself and/or groups of employees are to start using digital signatures, the government agency must enter into contracts for the procurement and maintenance of the necessary software and equipment, and have an agreement with a certification service provider. It is recommended that this should be based on the Public Administration Network Cooperation's framework agreements.

In order to obtain certificates, the government agency must have nominated one or more registration authorities or locations. The registration will normally be undertaken by people within the organisation, but this could also be a shared function for several government agencies. But the registration authority must be local, so that individuals who are to hold a certificate can get one by personally appearing, with identification documents, before the authority. The persons who are to act as registration authorities will need equipment and training, and must be approved by the certification service provider. If these are government employees, they will normally

be either technical, operational staff or employees in the human resources department. It is natural to tie the registration function to the human resources department. Employees there will need training particularly in the technical and security aspects of running such a service.

The use of digital signatures and message encryption must be reflected in the agency's security policy. A review of security policy is a natural step when introducing this technology. This should particularly involve a review of security for the persons and services that will use or verify digital signatures. Note that recommendations and regulations from *FO/S* and the Data Inspectorate, among others, require that each enterprise that uses cryptographic methods must appoint someone as head of encryption, with special responsibility for this area.

Use of digital signatures and certificates

The use of digital signatures and certificates can in itself be made quite simple. The challenge is to use them in the right context with electronic case processing and communication. This will require good documentation of new, tailored routines, followed by an adjustment process for introducing these routines. It seldom serves the purpose to transfer paper-based routines directly to electronic interactive ones.

The introduction of new routines may involve new roles and functions, and this may in turn involve some major administrative consequences, depending on the extent to which existing routines have to be changed. Examples arise particularly in the running and administration of services such as the receipt of electronic mail and electronic archiving.

The development of new electronic services, or the adjustment of existing services to suit the use of digital signatures, may involve altering operational procedures.

Building skills

Within the individual government agencies there are several types of employees who need special skills building. This obviously applies in particular to the users, who must know how to use smart cards and software, for example, and to know which routines apply to electronic case processing and communication. Changed routines may involve a significant need for training. This will be a necessary result of the change to electronic communication.

It is recommended that a programme of courses should be worked out based on courses already available in the field. Note that certification service providers and software suppliers who have framework agreements under the Public Administration Network Cooperation are obliged to offer user training courses to their clients.

The role of a registration authority is important and calls for special training. Both the equipment and the training of personnel who are to act as registration authorities must be covered by the contracts for the procurement of certificate services under the Public Administration Network Cooperation framework agreements.

Operations personnel in the government agency will need training in the installation, operation and maintenance of software and equipment (such as smart card readers). Operations personnel must also know any special security requirements relating to digital signatures and the encryption of messages that apply. Suppliers covered by the Public Administration Network Cooperation are obliged to give their clients such training, but it is recommended that Statskonsult or others should also prepare training courses.

13.4 Financial consequences

Broadly, the elements of a financial analysis are as follows:
- Expenses relating to the introduction of a common PKI,
- Expenses relating to the integration of digital signatures, etc., into existing and new systems,
- Financial savings linked to such an introduction.

This can to some extent be compared with:
- Costs of any alternative methods of achieving the same goals.

13.4.1 Costs of administrative measures

Joint administrative measures

The following administrative cost items can be anticipated. No attempt has been made here to quantify these points:
- Costs relating to the proposed coordination function, and to the Government administration's share in other coordinating actions, such as a common forum for government agencies, industry and suppliers to exchange experience,
- Costs relating to work on specifications, contracts, and administration, etc., of joint purchasing arrangements (the Public Administration Network Cooperation*)*
- Costs relating to international coordination,
- Costs relating to the development and implementation of skills enhancement measures – these costs can to some extent be passed on to the individual government agencies through participant fees, etc.
- Costs in the form of funds allocated to incentive measures from which money can be distributed to stimulate development in key areas in the community.

It has been stipulated that the coordination function ought to contribute 1-2 man-years of work to the secretariat, with an operating budget of NOK 6.5 million in the first year of operation (2001). It has been specified that each member of the coordinating committee will need to give two months' time to the work annually. A more substantial contribution will be required of the person who is to chair the committee. The Committee further proposes that the amount allocated in incentive payments should be NOK 9 million and that this should be administered by the coordinating function/committee. The proposal is for a grant totalling NOK 15.5 million from the government budget for measures that the Committee considers necessary to achieve

electronic 24/7 government administration in an acceptable way in 2003, the time limit that the Government has set.

Administrative actions within the individual government agencies

Reviewing and adjusting case processing routines and communication can be a very complicated and expensive job, but it is necessary if the advantages of using electronic communication and digital signatures are to be obtained. The complexity of the job will vary greatly from one government agency to another.

Once in operation, it should not normally demand significantly more resources than in a situation where digital signatures are not used. There will be certain additional responsibilities for operational staff, especially in relation to planning and internal measures, including responsibility for security of information, security procedures and PKI. The role of registration authority will not normally involve much extra work, but this of course depends on the size of the organisation, the number of persons who are to hold certificates and the frequency with which they are to be issued.

The training of users and the development of skills generally may involve considerable cost.

13.4.2 Costs involved in adapting PKI for the Government administration

The following items of government expenditure can be identified, in addition to the more administrative costs mentioned above:
- Procurement, maintenance and use of certificates, software and equipment (smart cards and card readers, etc.) for the Government's own use,
- Any contribution to the setting up of common services such as coordinated traffic services and directories,
- Any subsidy to the certification service providers in order to obtain services that suit the Government administration’s needs – see below,
- Each agency's costs relating to the use of certificates issued by commercial companies.

The latter item will amount to an expense relating to shared functions and can be assessed in relation to the administrative costs discussed above.

There is some basic data for calculating costs relating to the procurement and operation of the technology. This can be based on the price indications given by suppliers, on the maximum prices stated in the framework agreements of the Public Administration Network Cooperation and on calculations made by the Swedish authorities [32].

A general consideration is that two factors have a major impact on prices:
- The number of certificates issued and the number of software licences, smart cards, etc.,
- The number of services for which the certificates can be used, and the volume of traffic generated through these services.

Setting up a commercial certificate service is extremely expensive, and it is relatively costly to run. If the service is only to issue a few certificates, the cost per certificate will be high. At the same time, however, the market will hardly be willing to pay a high price for certificates, smart cards, etc.

The potential profit for service providers therefore does not lie in the PKI service itself, but in the income generated from new services that are made possible (or perhaps improved in quality) by using PKI and digital signatures. The costs of issuing certificates must to a large extent be covered by earnings from services offered. This in turn depends on the certificate issuer itself running these services or having contracts with service providers that secure a measure of financial compensation. Certification service providers can also have tariffs that are partly based on charges for the use of keys and certificates, and then the volume of use will be significant.

There is in fact good reason for claiming that the certification service providers in Norway must expect to lose money on the issue of certificates alone, given the certificate prices that one can expect the market to accept and the volume of business one can anticipate in Norway. The income will come from other services. A case in point is the banks, where BankID may be a tool for introducing profitable electronic banking services.

For the Government administration, this is yet another argument for relying on services procured commercially. The administration's own electronic services may be a reason in itself for acquiring certificates, etc. But the possibility of access to such services may be a very good additional argument for users who perhaps primarily wish to obtain certificates in order to access banking services, for example. This may well lead to better financial conditions for the Government than one could achieve by setting up a separate certificate service.

With a solution in which certificates, etc., are bought commercially from all players, the Government administration’s costs are in principle limited to its own procurement of certificates, software, smart cards and card readers.

Prices will depend to a great extent on volume, but a price of approximately NOK 1000 per installation seems likely (card reader, cards and certificate). Certificates will normally be changed every second year, while smart cards can have a life of two certificate periods, or four years. If we include an annual charge for certificates and the software maintenance costs, one can estimate a price of approximately NOK 2000 over a four-year period. With large volumes one can expect, as in other connections, to obtain discounts from the suppliers, with prices falling as the quantities purchased increase. Several suppliers have tariffs with volume discounts.

After this period, users will need new smart cards and one can anticipate the need for software upgrades, etc. One can therefore expect a further four-year cycle, probably with lower costs, on the assumption that PKI technology will by then have become mass market products.

Printing or other marking of cards as physical proof of identity, multi-purpose cards (applications other than electronic ID on the same card) and user support, etc., are not included in this calculation.

Given a certain volume of government procurement, it is not likely that the prices will be much higher than anticipated, and with a market breakthrough for PKI technology, the prices may well be lower.

Alternatives to smart card technology that one can imagine being used in suitable areas of the public administration services have anticipated prices that mean for example if an electronic ID is built into the software for net browsers, the price will be approximately 40% lower. Electronic ID in mobile telephones (i.e. use of a SIM card for storing keys) may be on the market as early as 2001, and it is expected that the price will be 20% lower than for smart cards. But such an ID will have limited use for signing documents.

It is hard to estimate the price per transaction when using digital signatures. Some suppliers anticipate that they will try a tariff under which they charge for the use of certificates and keys. The price structure here has not yet been settled. The processing of transactions with digital signatures is more complicated and expensive than without; among other things, it is necessary to check that the relevant certificate has not been withdrawn. Swedish estimates indicate NOK 5 per transaction, but this seems high. NOK 2.50 seems to be a more realistic estimate.

As far as certificates, software and smart cards for players in the private sector (industry, commerce and private individuals) are concerned, these players will in principle have to buy them commercially themselves. One must, however, be aware that the Government administration will be dependent on the available services maintaining a certain level. System integration will also involve costs for digital signatures.

Integration of software for digital signatures is a potentially complicated task. It must therefore the Government's goal to work out common specifications that minimise the degree of "tailoring" required for each individual service and software integration.

Much of the problem is related to coordinating traffic services and to handling certificates from different certification service providers. It is important to have standards for the format of certificates and to have solutions that avoid the need to make special adjustments for each individual service in order to be able to accept certificates from different certification service providers. Coordinated traffic services may be a valuable tool.

The suppliers included in the Public Administration Network Cooperation's framework agreements can already provide integration of digital signatures with a good choice of user software. Future specifications must focus on what the needs of the Government's users really are, and make sure that necessary integration is available commercially. One should be aware that there is a good chance that one will have to buy software for digital signatures and encryption from the same supplier that one has selected as the certification service provider, but there are also examples of general software that can deal with different kinds of certificates and smart cards.

Costs relating to system integration have not been quantified here. These are development costs that will probably be relatively high if such integration is to be carried out for each individual government agency.

13.4.3 Cost of alternative methods

There are at present no alternative standardised technologies that cover all the functions provided by digital signatures and PKI [66]. Possible alternatives are limited, specially adapted solutions. Seen in isolation, the costs of the first services and/or applications using digital signatures and PKI that are introduced will certainly be higher because one is at the same time working towards a general infrastructure instead of a solution for an individual service. It should nevertheless be reasonably clear that, viewed in relation to the extent to which digital signatures are expected to be used within just a few years, individual solutions are not very appropriate. It would mean that users would have to get an electronic ID for each service they wanted to use.

For authentication – where there is no explicit need for signatures – one can use passwords, from static passwords or PIN codes to various forms of one-time passwords such as are used in today's Internet banking. The best systems for one-time passwords do indeed provide as secure an authentication as PKI-based methods, and they support mobility. Experience shows that such solutions are relatively expensive. There is also the problem that users have to get hold of such a system for each service, and perhaps to remember a password for each service. This soon becomes unmanageable, especially when one looks at the whole spectrum of public and private services.

It is clear that the administrative costs of such solutions can easily reach very high levels, and the complexity increases the likelihood of errors. Password-based solutions simply do not match up to a combination of many services and many users. By the same token, neither do PKI-based solutions match up, if PKI is introduced without coordination.

13.4.4 Potential for reducing costs

The potential advantages of electronic services and electronic case processing are obvious, and the arguments will not be repeated here. The question that arises with the use of digital signatures and certificates is therefore what advantages they give to electronic services that could not be obtained without the use of PKI.

This report points out that there are services that should not be offered electronically without digital signatures, and that, in other cases, it is possible that the use of digital signatures might bring significant improvements in terms of quality. The report provides reasons indicating that these arguments are strong enough to justify the costs that are described in the foregoing paragraphs.

An important problem in connection with the use of PKI is the slow pace of bringing PKI into use. The spread of concrete solutions has so far proceeded slowly. Electronic public services are dependent on a certain volume of use if they are to be cost effective. Savings through more efficient (electronic) processing and a smaller volume of manual routines associated with paper processing must exceed the costs of offering the service electronically. There are at present few certificate holders within government administration, in industry and among private individuals. But great attention is being focussed on PKI and digital signatures, both in Norway and internationally. A great increase in the number of users is expected as the technology progressively gives access to more and better electronic services. One example is the banks' investment based on changes in the Act on financial contracts, which now allows the electronic signing of contracts and far more advanced electronic banking services than we have seen so far. Electronic services offered by the public sector may create a greater demand for certificate services. A number of public institutions are well ahead: the Directorate of Taxes and the National Insurance Administration, for example. For the public services, this is also a question of whether to seize the opportunity in terms of the number of users that can be attained in the short term.

The Committee makes no attempt to quantify the potential for reduced costs relating to making new electronic services accessible, and to improving the quality of other services, where these require digital signatures. This is linked to the advantages relating to the introduction of 24/7 government services. It is assumed that there is such a potential of not inconsiderable proportions. It is also assumed that in accordance with political aims the administration must be renewed and made more efficient within a reasonably short time (cf. The Renewal Programme, the eNorway Action Plan, 24/7 government services, etc.) and that this must be achieved in a sound and cost-effective way. It is in this context that the Committee's proposals are put forward.

13.5 Proposals that cost nothing?

A variation on the theme in the previous point is to look at the possibility of putting forward proposals that cost nothing in kroner and øre (at least not initially). A number of the Committee's proposals do not involve direct costs. They are recommendations that the individual enterprise, individual or firm can choose whether or not to follow. The consequences of such recommendations are difficult to quantify, but it is easy to imagine that they represent a type of adaptation that will save money because an individual enterprise can make use of solutions that have been carefully thought out centrally, rather than having to "re-invent the wheel" for itself.

Another possibility is to envisage the introduction and use of PKI solutions with and within the Government administration taking place without any coordination or preparation of any kind. This would probably lead to introduction and use based on the individual organisation's own approach and preparations. The largest departments and services do have the resources to do this, but the medium-sized and small ones will not be able to manage. After a time, PKI areas will probably emerge for individual enterprises, perhaps for whole sectors, probably with great differences in the choice of solutions and less potential for interaction between solutions.. One can

imagine this working satisfactorily for a time, but there is reason to believe that the usefulness will diminish in time as the obstacles to interaction become more apparent and problematic. It will probably be more demanding in terms of costs and resources for the individual enterprise to undertake the entire procedure for getting digital signatures (or alternative solutions) and encryption to work without the joint actions and preparation proposed by the Committee. The total cost of introducing electronic 24/7 government would probably be significantly higher for the Government as a whole.

Published by:
Ministry of Labour and Government
Administration, Norway

Additional copies may be ordered from:
Statens forvaltningstjeneste
Informasjonsforvaltning
E-mail: publikasjonsbestilling@ft.dep.no
Fax: + 47 22 24 27 86

Publication number: X-XXXX

Printed by: Ft - Hurtigtrykk/ - 11/2001