Preliminary Translation

Draft Bill

for

Act on Digital Signature etc.

PART 1
Scope and application

1. The purpose of the Act is to promote the secure and efficient utilization of digital communication by setting minimum requirements for certification authorities and digital signatures as well as the associated key certificates. A further purpose of the Act is to ensure an equal status of the possibilities of using paper-based and digital communication in all areas where digital communication may serve the same purpose as paper-based communication, and to make it obligatory for public authorities to be able to communicate digitally with all parties who wish so.

2.-(1) The Act shall apply to certification authorities and the key certificates issued by such authorities, linking a key pair for digital signature to a specific natural or legal person in such a manner that the addressee of a message provided with a digital signature, through the associated key certificate, may get proof of the sender's identity and be sure that the message originates from the sender in question and that the contents of the message have not subsequently been altered.

(2) The Act shall also apply to the digital communication of public authorities with natural and legal persons.

3.-(1) The Act shall not apply to payments transfer or payment transactions governed by the Act on Payment Cards.

(2) Integrated systems that may be used both for giving digital signatures and for payments transfer shall be arranged by the service provider in such a manner that it will be possible for the user in connection with each individual transaction to distinguish clearly between the two functions.

PART 2
Definitions

4.-(1) In this Act a key pair for digital signature shall mean a private and a publicly accessible signature key that are interdependent in such a way that a digital message that may be decoded by the publicly accessible signature key can only be encoded by means of the private signature key.

(2) In this Act a key certificate for a key pair shall mean a digital certificate which declares that a publicly accessible signature key in a key pair belongs to a specific natural or legal person.

(3) In this Act a digital signature shall mean the numerical value generated by the process of encoding a digital message by means of a system for digital signature and the private signature key in a key pair for digital signature.

(4) In this Act a certification authority shall mean natural or legal persons who issue and publish key certificates for digital signature.

(5) In this Act a keyholder shall mean a natural or legal person who has made an agreement with a certification authority on the issue of a key certificate.

(6) In this Act a time stamp shall mean a declaration indicating that a specific digital message existed at a specific time.

5.-(1) In this Act an authorized certification authority shall mean natural or legal persons who have been authorized by the National Telecom Agency to:

1) issue authorized key certificates, or
2) issue key certificates for authorized digital signature.

(2) In this Act an authorized key certificate shall mean a key certificate which is issued by an authorized certification authority and meets the minimum requirements for authorized key certificates in this Act or in regulations issued in pursuance thereof.

(3) In this Act a key certificate for authorized digital signature shall mean an authorized key certificate where signature keys and systems for giving digital signatures meet the minimum requirements for authorized digital signatures.

PART 3
Use of digital signatures

Note: At present this Part contains a description of three alternative models for implementing the fundamental equal status of digital and paper-based communication in relation to formal requirements for existence in writing and signatures. The intention is, on the basis of the hearing, to decide which model should be incorporated in the final Bill.

The exception model:

6A.-(1) Where Acts, provisions or regulations issued in pursuance hereof prescribe or stipulate that a message has to be given in writing or be signed, such requirements are considered to be satisfied when the message is given as a digital message with an authorized digital signature.

(2) The Minister responsible [following negotiation with the Minister of Research and Information Technology] may except Acts, provisions, regulations or parts thereof from subsection (1).

25a. Section 6A shall come into force on 1 January 2001.

The inclusion model:

6B. It may be laid down by Executive Order that Acts, provisions, administrative regulations or parts thereof which contain requirements for a message to be given in writing or be signed are considered to be satisfied by a digital message with an authorized digital signature.

The combination model:

6C.-(1) Where Acts, provisions or regulations issued in pursuance hereof prescribe or stipulate that a message has to be given in writing or be signed, such requirements are considered to be satisfied when the message is given as a digital message with an authorized digital signature.

(2) The Minister responsible [following negotiation with the Minister of Research and Information Technology] may except Acts, provisions, regulations or parts thereof from subsection (1).

25a.-(1) Section 6C shall come into force on 1 January 2001.

(2) It may be laid down by Executive Order that Acts, provisions, administrative regulations or parts thereof requiring a message to be given in writing or be signed are considered to be satisfied by a digital message with an authorized digital signature.

(3) Subsection (2) and Executive Orders issued in pursuance thereof shall be repealed with effect from 1 January 2001.

7.-(1) The holder of a key certificate may request the certification authority to bar the key certificate. Barring shall take effect when announced by the certification authority.

(2) No right can be based on a digital message with a digital signature where the associated key certificate is barred unless it is established that the digital signature was given before the key certificate was barred.

8.-(1) A key certificate may contain a time of expiry, subject to subsection (2).

(2) An authorized key certificate shall contain an expiry date, cf. section 15.

(3) No right can be based on a digital message with a digital signature where the associated key certificate has expired unless it can be established that the digital signature was given before the key certificate expired and that the digital message, before expiry of the key certificate, was supplied with a digital signature where the associated key certificate had not expired.

9.-(1) The key certificate may contain restrictions on the application area of the digital signature, subject to subsection (2)

(2) The Minister of Research and Information Technology shall lay down more detailed rules specifying what categories of restrictions on the application area may be used in connection with authorized key certificates and authorized digital signatures.

(3) No right can be based on a digital message with a digital signature where the message is outside the application area indicated in the key certificate.

Consequences of the expiry of a key certificate and violation of usage restrictions.

In sections 8(3) and 9(3), provisions are proposed for consequences in case of expiry and violation of restrictions on using digital signatures. The consequence has been formulated in such a manner that expiry and violation of the application area will have the result that no right can be based on digital messages with a digital signature.

This consequence seems appropriate in connection with the barring situation (section 6(2)), where the private signature key in some way or the other comes into the possession of an unauthorized third party, or the keyholder has lost control of his private signature key in other ways.

However, on expiry of the key certificate and violation of usage restrictions, the keyholder will typically still have control of the private signature key in question. It will be more likely for the keyholder to have forgotten or overlooked the expiry or usage restriction. So there might be situations in which the keyholder had intended to commit himself according to the contents of the message. In this situation, because of the formulation of the liability rule, the keyholder might later choose to disclaim an offer, referring to the fact that the key certificate had expired or the message was outside the application area of the key certificate. On the other hand, the stipulated rule is clear and unambiguous - also to those who receive a signature.

Instead it would be possible to formulate the rule on consequences as a rule shifting the burden of proof so that no right can be based on the signature unless it is established that the keyholder intended to commit himself according to the contents of the message. In the case of expiry of the key certificate, a rule shifting the burden of proof should be supplemented with a requirement to establish that the signature is still secure. If such reversed burden of proof is chosen, the decision will ultimately lie with the courts.

If it is maintained that no right can be based on a digital signature given after the expiry date, it should be considered to replace the requirement for affixing a "fresh" digital signature before the expiry date with a rule shifting the burden of proof, so that the addressee is to prove that the document has not subsequently been tampered with. Such rule will probably be more expedient in practical life. On the other hand, administration of the rule is not equally easy.

Which of the models should be incorporated in the Bill?

10. At the request of an addressee, certification authorities shall give information on the following:
1) any barring introduced,
2) any expiry date applicable, and
3) any restrictions on the application area.

11.-(1) A certification authority shall compensate keyholders and addressees of digital signatures for any loss due to failure of the certification authority to observe its own security regulations as well as the rules of section 3(2), section 7, section 10 and section 12, subject to subsection (3).

(2) A certification authority authorized under section 14(1), no. 1, shall compensate keyholders and addressees of digital signatures for any loss as mentioned in subsection (1) as well as any loss due to failure of the certification authority to observe the provisions of section 15 and regulations issued in pursuance of section 14(3).

(3) A certification authority authorized under section 14(1), no. 2, shall also pay compensation for any loss due to failure to observe rules issued in pursuance of section 14(6). If such loss can be ascribed to the keyholder's negligence, the liability to pay compensation to the keyholder may be reduced or cease, and the certification authority may have recourse against the keyholder for any compensation paid to addressees.

(4) The certification authority's liability to pay compensation under subsections (1)-(3) shall cease if the digital signature is given after expiry or barring of the key certificate, or in case the digital signature is given on a digital message not included under the application area as indicated in the key certificate.

(5) Subsections (1)-(3) may not be departed from by previous agreement to the detriment of the injured person or the party subrogating to the injured person's claim.

(6) Any loss not included under subsections (1)-(4) shall be regulated by the general compensation rules of Danish law.

PART 4
Certification authorities

12.-(1) On request, certification authorities shall give information to anyone about the certification authority's certification practice and other business terms. As a minimum, this information shall contain a description of the certification authority's procedures for issuing key certificates, including the certification authority's rules for verifying the identity of the keyholder, the certification authority's internal security procedures etc.

(2) On request, certification authorities shall also give information to anyone about the following:

1) How the digital signature is used.
2) Terms connected with holding and using a key certificate, including requirements for storing and protection of the associated private signature key.
3) The user's cost of obtaining and using a key certificate and using the other services of the certification authority.
4) The certification authority's and the keyholder's liability for loss in connection with the use of digital signatures.
5) How the keyholder should notify the certification authority with a view to barring in case the private signature key or an authorization code associated therewith is lost, misused or comes into the possession of other parties.

13.-(1) Unless otherwise stipulated under this Act, the Act on Data Protection etc. shall apply to the handling of personal data in connection with the operation of the certification authority.

(2) The certification authority may not use data on keyholders for purposes other than those connected with the operation of the certification authority. The certification authority may not pass on data on keyholders other than data appearing from the key certificate.

(3) Data showing who has looked up in the database of the authorized certification authority may only be used or passed on if this is necessary for implementing digital signatures, law enforcement or when authorized under other Acts.

14.-(1) On application, the National Telecom Agency may grant authorization to natural and legal persons to:

1) issue authorized key certificates, or
2) issue key certificates for authorized digital signature.

(2) An authorization may be revoked.

(3) The Minister of Research and Information Technology shall lay down rules specifying the conditions for obtaining the authorization as a certification authority, including application requirements and rules for revoking an authorization granted.

(4) In provisions under subsection (3), requirements may be stipulated for the following aspects:

1) capital basis
2) physical and logical security
3) emergency preparedness

(5) Provisions under subsection (3) shall also include requirements for the certification authority's procedures for:

1) verifying the identity and registration of the keyholder and the keyholder's public key,
2) issuing key certificates,
3) setting up and operating a database for key certificates,
4) barring of key certificates, and
5) provision of facilities for the purpose of time stamping.

(6) Provisions under subsection (3) dealing with authorization as mentioned in subsection (1), no. 2, shall also contain requirements for the certification authority regarding the technical and security-related requirements to be met by the systems that may be used for giving authorized digital signatures. On the basis of this the certification authority may stipulate requirements for the system(s) to be used by the keyholder for giving authorized digital signatures and for the expiry date thereof.

The supervisory authority's publication of authorized certification authorities

Is it necessary for the supervisory authority to issue certificates to certification authorities, or will it be sufficient that the certificates of the certification authorities be identified in other ways - e.g. through publication of certificate fingerprints in newspapers, the Official Gazette etc? An electronic hierarchy where the supervisory authority is issuing certificates to certification authorities will imply that the supervisory authority can apply for inclusion of the central key in the browsers existing in the market so that these may automatically recognize certificates issued under a Danish supervisory authority rather than a situation where individual certification authorities would have to apply for inclusion to browser producers.

On the other hand, the establishment of a Danish supervisory authority with a central key will be much more costly than publication in other ways (off-line), and over time these costs will have to be imposed on certification authorities. It will therefore be desirable to have information on how the market looks at this question.

15. An authorized key certificate shall contain the following:
1) unique identification of the keyholder,
2) activation and expiry date of the key certificate for digital signature,
3) information indicating that the key certificate is authorized and whether the digital signature is authorized, and
4) information on any restrictions on the application area.

16. The Minister of Research and Information Technology may lay down rules for fulfilling international agreements on mutual recognition of certification authorities, key certificates and digital signatures ensuring that foreign key certificates which meet the requirements for authorized digital signature under this Act may be used for giving authorized digital signatures.

PART 5
Duty of public authorities to use digital communication

17.-(1) Public authorities and institutions etc. governed by the Public Administration Act, cf. section 1(1) and (2) thereof, shall offer private individuals digital communication with public authorities.

(2) The Minister of Research and Information Technology shall lay down more detailed rules for this.

(3) Natural persons who generally want to receive messages from public authorities and institutions in a digital form may notify an e-mail address to the civil registration system (CPR).

(4) Legal persons registered in the central business register (CVR) and who generally want to receive messages from public authorities and institutions in a digital form may notify an e-mail address to this register.

Section 17(2): This provision makes it possible to lay down restrictions as to what documents authorities etc. are to receive. Should it be decided instead by the individual authority or institution what document formats it wants to receive?

PART 6
Supervision etc.

18.-(1) The National Telecom Agency shall maintain supervision to ensure that certification authorities comply with the rules of section 3(2), section 7, section 10 and section 12.

(2) Furthermore the National Telecom Agency shall maintain supervision to ensure that authorized certification authorities under this Act comply with the rules of section 15 and regulations issued in pursuance of section 14(3).

(3) The National Telecom Agency shall lay down regulations on the establishment of a system auditing unit and how to carry out system auditing.

(4) The National Telecom Agency shall make decisions regarding failure to comply with the provisions of subsections (1) and (2). However, the National Telecom Agency may not deal with questions of compensation. In connection with the decision of a case the National Telecom Agency may issue orders to certification authorities.

(5) The National Telecom Agency may impose daily penalties on a certification authority for the purpose of enforcing compliance with orders as mentioned in subsection (4). Distraint may be levied to recover the amounts.

(6) The National Telecom Agency may revoke a certification authority's authorization in case the certification authority fails to comply with orders as mentioned in subsection (4) and in case an authorized certification authority fails to pay daily penalties imposed under subsection (5).

19.-(1) The National Telecom Agency may demand all such information from authorized certification authorities as is deemed necessary for administration of this Act and rules issued in pursuance thereof.

(2) The National Telecom Agency may at any time, subject to proof of its identity and without a court order, make inspection visits at the business address of an authorized certification authority.

20. The Minister of Research and Information Technology may decide that authorized certification authorities should pay a fee for the case administration involved in the authorization, for the supervision maintained under section 18, and for other public expenses necessary for the Minister of Research and Information Technology to exercise his powers under the Act. The fee may also include expenses associated with the Appeals Board referred to in section 21.

PART 7
Complaints

21.-(1) Complaints regarding the decisions of the National Telecom Agency in pursuance of section 18(4)-(6) and section 19 or regarding the National Telecom Agency's case administration in connection therewith may be brought before an

Appeals Board appointed by the Minister of Research and Information Technology. The Appeals Board cannot make decisions in matters regarding compensation. In connection with a decision, the Appeals Board can issue orders to a certification authority.

(2) The Appeals Board shall consist of a chairman, who is to fulfil the ordinary conditions for being a High Court judge, and four members who, collectively, must represent the necessary expertise in technical, financial and consumer fields.

(3) The chairman and members shall be appointed by the Minister of Research and Information Technology for periods of three years. Reappointment shall be possible.

22.-(1) The Appeals Board may impose daily penalties on a certification authority for the purpose of enforcing compliance with orders, cf. section 21. Distraint may be levied to recover the amounts.

(2) The Appeals Board may direct the National Telecom Agency to revoke authorizations:

1) if an authorized certification authority fails to comply with orders as mentioned in section 18(1), and
2) if an authorized certification authority fails to pay daily penalties as mentioned in subsection (1).

(3) The Appeals Board may request the National Telecom Agency to give technical assistance for the purpose of carrying out investigations for elucidation of a case, or may request such assistance from other parties.

(4) The Minister of Research and Information Technology shall lay down more detailed rules for the activities and case administration of the Appeals Board, including rules on the following:

1) collection of fees for cases dealt with by the Board,
2) time limits for submitting complaints to the Board.

(5) The Minister of Research and Information Technology shall bear the costs of secretarial assistance to the Board, subject to section 20.

23.-(1) The decision of the Appeals Board cannot be referred to other administrative authorities.

(2) The decision of the Appeals Board may be brought before the courts for a period of up to six weeks after the date on which the decision was communicated to the parties involved.

(3) If a certification authority fails to comply with the decision of the Appeals Board and has not brought the decision before the courts within the time limit referred to in subsection (2), the Appeals Board may impose daily penalties on the certification authority. Distraint may be levied to recover the amounts.

(4) Subject to recommendation by the Appeals Board, the Minister of Research and Information Technology may furthermore revoke the authorization of the certification authority.

PART 8
Sanctions etc.

24.-(1) Unless more severe punishment is prescribed under other laws, any person who wilfully gives wrong information to, or fraudulently withholds information from, a certification authority in connection with the issue of a key certificate shall be liable to a fine, simple detention or under aggravated circumstances imprisonment for up to six months.

(2) Companies etc. (legal persons) may be held criminally liable under the rules of Part 5 of the Danish Criminal Code.

PART 9
Coming into force etc.

25.-(1) This Act shall come into force on 1 January 1999, subject to subsections (2)-(4).

(2) Section 17(1) shall come into force subject to further decision by the Minister of Research and Information Technology, but not earlier than 1 January 2001.

(3) Section 17(3) shall come into force subject to further decision by the Minister of Research and Information Technology.

(4) Section 17(4) shall come into force subject to further decision by the Minister of Research and Information Technology.

26. This Act shall not apply to Greenland and the Faroe Islands but may by Royal Order by put into force for these parts of the Kingdom with such modifications as may be required by the special conditions prevailing in Greenland and the Faroe Islands.

General Comments

A. Existing rules

The rapid development in recent years within the field of information technology, including the merging of electronic data processing and telecommunications, has led to an increased use of digital communication in all spheres of society. The use of electronic mail and information exchange via the Internet is rising sharply. Within the business community, the technology is being used increasingly for electronic commerce, i.e. for making contracts and transferring payments via electronic media, including the automatic exchange of business documents such as orders and invoices (e.g. via EDI - Electronic Document Interchange). For example, 80% of all Danish companies with more than 5 employees are today exchanging data electronically with other companies or with public authorities.

In relation to public authorities, electronic communication enables more efficient communication between authorities and private citizens and companies. For example, electronic self-service systems are being developed which allow the citizen to file his tax return, applications etc. from a home PC or from a public information kiosk. In the long term, digital communication will also enable citizens to have access to files under open public administration.

Today, electronic exchange of data between companies is carried out in dedicated systems where a specific code of practice, i.e. legal effects, security aspects, exchange formats etc., has been agreed in advance between the parties involved. The common standards for electronic data interchange currently being implemented by the central organizations of the Danish corporate sector as an element of a national EDI action plan may serve as an example of a code of practice used in such dedicated systems. Companies frequently doing business with each other have found it useful to set up such framework agreements.

However, this solution is not feasible if it is desired, in principle, that all companies, authorities and private individuals on the network should be able to carry out legally binding transactions mutually, for example placing an individual order or enter into an individual agreement whether or not they have been in contact with each other before.

As a result, there is a growing demand by the commercial sector for legal regulation that may provide a satisfactory framework ensuring that it will be possible to make legally binding transactions via open networks such as the Internet without having to arrange with the addressee in advance how to do it.

However, the Danish business community is not the only sector to be interested in electronic communication. It is to be expected that the use of the Internet by private individuals in a commercial context, i.e. ordering and buying goods via the Internet, will grow dramatically.

For private citizens it will also be relevant to use the Internet to file tax information, apply for loans, order medical cards, passports or driving licences, file building licence applications or notify change of address, or receive electronic prescriptions from their doctor following up on a telephone consultation etc.

The use of electronic communication for binding legal transactions presupposes that it is possible to communicate with security of the sender's and the addressee's identity, the integrity of the content, and often with guaranteed confidentiality in relation to other parties as well. In other words, solid technical solutions must be available.

When we communicate on paper, our signature and letter paper serve to identify us to the addressee, who will also be able to see if the envelope has been opened in transit and whether alterations have been made in the written text. In practice, communication is usually exchanged without much thought being given to these aspects. And in fact it is only in a few exceptional cases that we need to pay attention to it.

When communication is electronic, there is no concrete evidence in the same manner which makes us notice immediately that the content of a message may have been altered, and it is difficult, not to say impossible, to be sure who is the actual sender of the message. This means that in practice it is much easier to make alterations in a message or pretend to be another person without this being visible to the addressee.

A solid digital signature may safeguard against these problems. The use of digital signatures calls for a special infrastructure to ensure the user of such signatures the capability of verifying the originator's identity and to provide security to the originator as well as the addressee with regard to the integrity of the content.

For this purpose it will be necessary to set up one or more establishments known as certification authorities which may act as independent third parties for verifying identities. In principle, it might be left to the market itself to arrange for certification authorities to be established and to ensure that the solutions they offer will be solid enough. But this is a new market with products of such technical complexity that it is extremely difficult for the individual user to be sure that the product offered has the necessary security.

The purpose of the present Bill is to regulate the activities of certification authorities by way of an authorization scheme and a number of minimum requirements for the security of certification authorities as well as a number of requirements for the design, security level etc. of digital signatures which may promote the provision of solutions

having the necessary quality. Furthermore the purpose of the Bill is to define the extent to which the certification authority is liable in connection with faults and misuse of digital signatures.

Besides the uncertainty as to what systems for digital signature are secure, there is uncertainty about the possibility of using digital communication and digital signatures for legally binding transactions. What can you use a digital signature for, and with what legal effect?

In a number of fields there are no formal requirements in Danish law, i.e. no requirements for a specific legal transaction to be made in writing, be signed etc., in order for the transaction to be regarded as valid and binding. This applies for instance to formation of ordinary business contracts. In such areas the decision as to whether a digital signature is proof that a specific person has signed a specific message will ultimately lie with the courts. As in the case of a handwritten signature, the courts are to make a concrete decision in each individual case as to whether a signature has been given by the person it purports to represent and whether the document has subsequently been altered. The starting point here - as in the case of ordinary signatures - is that the courts have freedom to assess evidence, including freedom to assess the concrete evidence produced in support of the authenticity of the individual digital signature(s).

With framework legislation on digital signatures, which - as mentioned above - will ensure solid systems, it may be expected that an authorized digital signature given in conformity with the requirements of the law will have great evidential weight in connection with a lawsuit.

The question is, however, whether the courts will accept digital signatures immediately in areas where there are special statutory requirements for signature and existence in writing etc. Irrespective of legislation on digital signatures it must be considered doubtful whether electronic communication will be accepted in all cases in areas with such formal requirements. Some formal requirements may be fulfilled by digital communication, while there may be other areas in which digital communication cannot be applied for various reasons.

This legal uncertainty is not desirable, considering the socioeconomic advantages of furthering electronic communication. It should be clear to citizens in what areas, to what extent and in what way it is possible to use digital communication with digital signatures when there are formal requirements for existence in writing or signatures. In other words, it must appear clearly where you can and where you cannot, communicate digitally.

The equal status of digital and paper-based communication cannot be implemented in all areas. There may be areas not yet suitable for digital communication because the

digital world does not yet offer the same functionality as we have today with paper-based communication. In the same way, there may be other aspects which imply that it will not be possible to use digital communication in the short term.

An overall review of all legislation and regulation through Executive Orders are to clarify whether and to what extent it will be possible in each individual area to use digital communication.

The hearing version of the Bill contains three alternative models on how the equal status of digital and paper-based communication may be implemented in practice. The intention is, on the basis of replies to the hearing etc., to make the final choice between these three models. See also section C(2) and sections 5A-C of the Bill.

B. Background

1. What is a digital signature?

A digital signature is a numerical value giving the same function as an ordinary handwritten signature, i.e. relating a certain amount of information to a specific person. In addition, a digital signature provides security that the signed message cannot be altered subsequently. A digital signature is produced by means of a computer program based on the use of encryption techniques.

A digital signature is created by means of a secret code known as the private signature key, which is only accessible to the user concerned. The private signature key is associated with a publicly accessible code known as the public signature key, which may be used by others to verify the digital signature, i.e. verify the sender's integrity and the integrity of the message. This is because the private signature key and the public signature key are interrelated in such a manner that a digital message which may be decoded by means of the public signature key can only have been encoded by means of the private signature key.

In itself the signature does not mean anything to the addressee since it appears as a group of apparently random letters and digits, but by applying the sender's public signature key to the signature, the addressee's computer program can determine whether the signature was given by means of the sender's private signature key. If the sender's public signature key can decode the signature, the signature has been verified.

Example:

If a patient communicates electronically with his doctor, the patient wants to be sure that e.g. a prescription originates from the doctor and nobody else. By using his private signature key to sign the prescription, the doctor provides this security to the patient. The patient may obtain the doctor's public signature key from the certification authority and have the doctor's signature verified. The patient can now be sure that it is the doctor who has given the prescription.

The system is also important in other areas, e.g. electronic agreements: The seller is willing to send his goods to the customer, confident that the order in fact originates from the customer and not from an unauthorized third party.

Digital signatures may also be used by legal persons (e.g. a company such as Lego A/S). If a company is using a digital signature, it will be comparable with digital letter paper, where the addressee will have proof that the message originates from that legal person. Combined with a digital signature from a natural person who is entitled to sign for the company in question, the digital letter paper may serve as a basis for a message indicating, for example, that Peter Hansen, Product Manager of Lego A/S, wants to order 10 new PCs for installation in week no. 23.

Digital signature with fingerprints

The calculations to be made for digital signatures are quite complicated - so complicated in fact that they will occupy an excessive amount of computer power if the documents to be signed have a certain and not very large extent. To reduce this problem, most programs for digital signature are designed in such a way that they generate what might be called fingerprints of the text (also known as a hash value), which is encoded by means of the private signature key. By signing the fingerprint instead of the whole document, resource savings are obtained. The fingerprint is generated in a way which gives a high degree of security that two different texts will not have the same fingerprints.

The consequence of using techniques with fingerprints is that a digital message with a digital signature will consist partly of the message itself in plain text (not encoded) and partly the fingerprint of the message encoded by the originator's private signature key. The fingerprint in an encoded form is the digital signature.

The addressee decodes the fingerprint using the sender's public signature key, and may now compare the decoded fingerprint with the fingerprint of the message itself, calculated by his own computer. If the two fingerprints are identical, then the signature was given by the person indicated as the keyholder in the key certificate.

2. Digital signature in practice

To generate a digital signature, it is necessary to have a private signature key and a computer program which, on the basis of the signature key and the digital message, can make the calculations for the digital signature.

In most cases the private signature key is generated by the computer system that the user wants to apply for calculating the signature. This may be for example a browser, the newest versions providing the capability of generating digital signatures. When the key has been generated by the user, it will typically be stored on the user's PC. If ready-made solutions are bought, e.g. homebanking etc., the key may be generated by the program supplier, and the signature key can be delivered on diskette or CD-ROM or other portable storage media. In the long term it must be expected that chipcard solutions will be offered, where a user may buy a chipcard and the key is generated and stored on the chipcard. This solution is the most secure solution known for storing keys since the chipcard is difficult to tamper with.

The private signature key is to be protected by a PIN code or password, known from the "Dancard"[1] and PCs. Thus the keyholder will activate his private signature key by keying his PIN code. This will protect against unauthorized use of the key if an unauthorized third party comes into possession of the medium on which the key is stored. Like the Dancard, the user's handling of his PIN code is therefore an essential security factor in a digital signature system.

With a private signature key and a computer program, it is possible to give digital signatures. However, if the signature is to be governed by this Bill, it is a precondition that the public key should be registered at a certification authority. Thus the certification authority plays a decisive part in an infrastructure for digital signatures. The chief task of the certification authority is to ensure the addressee of a digital signature the capability of verifying the originator's identity. In other words, the certification authority is to declare what natural or legal person a key pair for digital signature belongs to.

To this end, the certification authority will issue a key certificate, i.e. a data file containing the keyholder's name, address or other information identifying the holder, as well as the keyholder's public signature key. The addressee's PC will check automatically whether the digital signature may be verified by means of the public signature key in the key certificate. If this decoding is successful, the addressee can be sure that the message was originated by the relevant natural or legal person stated in the certificate, and that the message has not subsequently been altered.

---

[1] Danish electronic payment card system.

In addition, the addressee must ensure that a number of conditions have been fulfilled. In the first place, the addressee must examine whether the key certificate is barred. This may be the case if the keyholder has lost control of his private key. Secondly, the addressee must examine whether the key certificate has expired. Finally, the addressee must examine whether there are restrictions on the digital signature in the associated key certificate and, if so, examine whether the digital message falls within or outside the application area.

Barring of a key certificate will occur for example in connection with misuse or loss of control of the private signature key. If the key certificate is barred, no right can be based on the digital signature unless it was given before barring was announced by the certification authority. The certification authority may notify users of barred key certificates in several ways, but it is required that information as to whether a key certificate is barred or not must be available to all potential addressees. Barring is discussed in further detail under section C(1).

If an expiry date is fixed for a key certificate, this must appear from the certificate. A key certificate might for example be valid from 1 January 1998 to 1 January 2001. The consequence of a key certificate expiring is that no right can be based on digital signatures given after the expiry date. Thus it will not be possible to base any right on a digital signature given after 1 January 2001. Expiry is discussed in further detail under section C(1).

The application area will appear from the key certificate. A digital signature may for instance be restricted to be applicable for certain transactions only, e.g. communication with public authorities or for homebanking etc. In case a message with a digital signature falls outside the application area in the key certificate, no right can be based on the message. Barring is discussed in further detail under section C(1).

It is the addressee's risk to rely on a digital signature without having examined the conditions mentioned. If the addressee omits to verify a signature and it turns out that the key certificate had expired or was barred, the addressee will have to bear any loss in connection with this.

C. Content of the Bill

The Bill is based on a number of expert reports on legal problems in connection with the introduction of systems for encryption on open networks, including the National Telecom Agency's "Main Report on a Possible Authority Initiative in the Encryption Area", dated June 1993, and the IT Security Council's proposal for "Denmark's IT Security Policy", issued in November 1996.

While drafting the Bill, the Ministry of Research and Information Technology has also had several consultations with the sectors and organizations most affected, in order to ensure the technical foundation of the Bill and to take relevant interests into consideration at an early stage.

In December 1997, the Minister of Research and Information Technology, together with the Minister of Business and Industry, the Minister of Economic Affairs and the Minister of Taxation, gave a report to the Folketing (the Danish parliament) on the security of digital communications, including digital signature.

The Bill contains the following principal elements:

1. Authorization scheme for certification authorities
   a. Expiry of key certificates
   b. Barring of key certificates
   c. Restrictions on the use of digital signatures
   d. Liability
2. Regulation of formal requirements for existence in writing and signatures
3. Duty of public authorities to be able to receive digital communication
   a. Document formats

1. Authorization scheme for certification authorities

The purpose of the Bill is to promote the secure and efficient utilization of digital communication by setting a number of minimum requirements for certification authorities and key certificates issued by certification authorities.

The Bill comprises certification authorities without an authorization, as well as certification authorities with an authorization. The Bill stipulates a few requirements applicable to all certification authorities as well as a number of more extensive requirements for certification authorities that wish to obtain an authorization.

Any certification authority must publish its certification practice and other business terms. As a minimum, this information must give a description of the certification authority's procedures for issuing key certificates, including the authority's rules for verifying the keyholder's identity, the authority's internal security procedures etc. This certification practice is also of importance to the liability of certification authorities to pay compensation, see comments on section C(1).

A certification authority may apply for authorization for the purpose of issuing authorized key certificates or for the purpose of issuing key certificates for authorized digital signatures.

The two authorization models represent two different security levels. While the certification authority issuing authorized key certificates is solely guaranteeing security on and in connection with the key certificate, the certification authority issuing key certificates for authorized digital signatures is also guaranteeing security in the computer system and the signature key employed by the keyholder.

The two authorization models thus differ only in that the certification authority issuing key certificates for authorized digital signatures undertakes a guarantee to addressees for the software that the originator is using for generating keys and affixing authorized digital signatures.

In the nature of the case it will primarily be in connection with authorized digital signatures that there will be a prior assumption that the courts will consider such digital signatures secure. For the same reason, only authorized digital signatures may thus be used in areas where the law contains formal requirements for existence in writing or signatures. This is because only authorized digital signatures give a guarantee to the addressee that all elements in the creation of the digital signature meet the minimum requirements for secure digital communication.

Authorized key certificates give a guarantee to the addressee that adequate identification of the keyholder has been made, but there is no guarantee that the keyholder is keeping his key in a safe way, just as there is no guarantee that the keyholder's software for generating digital signatures meets the security requirements. As a consequence, an authorized key certificate does not entail the same prior assumption of acceptance by the courts, nor does an authorized key certificate fulfil formal requirements for signature and existence in writing.

But an authorized key certificate guarantees that the certification authority fulfils the security requirements of the Bill for identification of the keyholder, issue of key certificates, publication of barring notices etc.

Furthermore an authorized key certificate must contain information stating that the key certificate is authorized, its expiry date, any restrictions on its use as well as information indicating whether it is issued for authorized digital signatures.

a. Expiry of key certificates

A certificate for digital signature will have a limited lifetime. A signature key described as secure today may not necessarily be secure in ten years, considering the explosive development of the computing power of PCs. It must therefore be expected that signature keys will become obsolete and that after a number of years digital signatures already given may be exposed to forgery.

Users must therefore be prepared to obtain new key certificates with new and better signature keys gradually as the signature keys can no longer be regarded to protect sufficiently against manipulation.

The Bill requires certification authorities issuing key certificates for authorized digital signatures to indicate an expiry date in the certificate. The certification authority guarantees that the signature key is secure until the expiry date.

When a key certificate has expired, no right can be based on a digital message with a digital signature unless it is established that the digital signature was given before the key certificate expired and that the digital message was supplied, before expiry of the key certificate, with a digital signature where the associated key certificate had not expired.

This supplementary digital signature or "refreshment" will thus have to be given on the message before expiry of the key certificate. In case a supplementary digital signature is not given in time before expiry of the key certificate, no right may be based on the message. In other words, there must always be a digital signature on a document where the associated key certificate has not expired.

As indicated in the question box in the Bill itself directly after section 9 of the Bill, this is a rather hard-and-fast rule, which might advantageously be replaced by a reversed burden of proof.

This expiry problem illustrates that the digital technique is much different from the paper handling we have got used to over several hundred years. Thus it will be necessary to keep an eye on the validity of digital documents that are of significance over a longer period of time.

b. Barring of key certificates

The keyholder may request the certification authority to bar a key certificate, for example because an unauthorized third party has got access to the keyholder's private signature key. No right can be based on digital signatures given after the time of barring.

This poses two questions:

The first one is the question as to how the certification authority should notify addressees of digital signatures that the key certificate is barred. The Bill makes it obligatory for certification authorities to notify addressees of barring in connection with

the verification. The obligation may be met for example by the certification authority setting up a database of all certificates issued and inserting notes on barred certificates.

The next question is whether a digital signature was given before or after the time of barring. This determination is decisive because barring takes effect when notification thereof has been published by the certification authority. The decision as to when a digital signature was given may also be of significance in connection with a supplementary digital signature to be given before expiry of a key certificate, see comments on the expiry of key certificates above.

The time of giving a digital signature will not necessarily appear from the signature itself. The signed digital message itself may contain a date.

It may be possible to determine the time by going through log files on the originator's computer system, although such dating may be manipulated by the originator. If the message has been sent via open networks, it may be possible, by going through the log files of a third party who has transported the message to the addressee (e.g. an Internet provider), to ascertain when the message was sent and received respectively.

In practice, however, it will often be technically difficult to determine the time when the digital signature was given.

A solution to these evidence problems may be to let the message with a digital signature or merely the signature itself be time stamped by an independent third party. It is only necessary to time stamp the signature itself as it may be verified later that the signature is associated exclusively with the message in question and that the message has not been altered, see the description of digital signatures under section B. Time stamping may be made via a certification authority or another independent institution which will affix a time stamp to the message or signature.

It has been considered whether it should be obligatory for the originator to time stamp a message with a digital signature, thus ensuring that it is determined in all situations when a transaction was made. However, there will be a number of situations in which time stamping is not considered necessary, either to the originator or the addressee, and there may also be situations in which it is primarily the addressee who needs, via independent time stamping, to be able to prove when a digital signature was originated or received. Whether the originator or the addressee chooses time stamping will thus be governed by their legal interest in such stamping and their need for it. As a result, the Bill does not contain specific regulation indicating in what situations the originator and addressee respectively are to use time stamping.

Time stamping may also be relevant where the sender or addressee subsequently wants to be able to document the time of sending, respectively receiving, a document.

An authorized certification authority is to provide or arrange an offer for a time stamping service.

c. Restrictions on the use of digital signatures

Digital signatures represent an entirely new and unknown technique to most people. Some familiarization will probably be needed before everyone has full confidence in these systems. It may therefore be desirable, both for users and certification authorities, that there should be an opportunity to test the system. It may be, for example, that a user is interested in buying goods via the Internet, but does not want to be able to sell his house using his digital signature. Or that the user is interested in being able to file his tax return etc. with public authorities, but wants no access to electronic commerce. In the same manner, it may be relevant for the certification authority to restrict the use of the certificate in order to control the risk of losses due to misuse, for which the certification authority is liable. Thus the certification authority may limit its activities to a smaller area or merely build up its activities over time.

Restrictions on the application area will appear from the key certificate. Addressees of digital signatures will therefore become aware of the restriction in connection with the verification of the signature if the addressee examines the content of the key certificate.

If a digital message with a digital signature falls outside the application area, no right can be based on the digital message in question.

Restrictions on the use of a key certificate may involve problems if the restriction is described in such a manner that it is not immediately clear to the addressee whether the use falls within the application area. As a result, the Bill contains authority for the Minister of Research and Information Technology to lay down a number of categories for authorized key certificates.

d. Liability

The Bill embodies regulation for the liability of certification authorities and keyholders.

Certification authorities have absolute liability towards keyholders as well as addressees of signatures for any loss due to failure by the certification authority to observe its own regulations.

A certification authority issuing authorized key certificates also has absolute liability for observing the minimum requirements laid down pursuant to the Bill for authorized key

certificates. This includes a number of security procedures regarding identification of users, key generating, issuance and handling, including any barring of key certificates.

A certification authority issuing key certificates for authorized digital signatures is also liable for ensuring that the security of the systems employed by the user to give digital signatures observe the minimum security requirements of the Bill. This means that the certification authority, based on the minimum requirements of the Bill, may prescribe what systems the user should employ for digital signatures and how long the certification authority guarantees the key certificate. If these systems cannot live up to the stipulated minimum requirements, the certification authority has to pay compensation for any resulting loss, see section 11(3).

However, if the certification authority demonstrates that this loss is ascribable to the keyholder's negligence, the liability of the certification authority towards the keyholder may be reduced or cease, and the certification authority may have recourse against the keyholder for any compensation paid to addressees. The situations in which the keyholder has a share in the liability, are concerned with protection of the private signature key and use of the software prescribed by the certification authority.

The proposed liability of the certification authority for the user's choice of software for digital signatures is rather extensive since the certification authority is not really in a position to ensure that the user in fact employs the software that the certification authority has required him to use. As a result, the Bill contains the possibility of shifting the absolute liability to the keyholder in situations where he is responsible for a specific fault, for example through failure to employ the prescribed software or by having shown negligence in handling the private signature key.

The reason for this liability regulation is primarily that the security of an authorized digital signature would be illusory in practice if the routines of the certification authority and the software employed are not both included under the security scheme and the liability of the certification authority. If an authorized digital signature is to be recognized by the courts, it must be required that all security critical elements in the digital signature are included under the scheme.

Obviously this will place a heavy burden on the certification authority, and the Ministry of Research and Information Technology would be glad to receive proposals for other solution models which may offer the same guarantee that an innocent addressee of an authorized digital signature may be compensated for loss due to breach of statutory security and quality requirements.

If neither the certification authority nor the keyholder has committed any fault, the liability to pay compensation must be decided according to the ordinary compensation rules of Danish law.

In case of forgery, the ordinary rules of Danish law will be applicable. This means that the Bill does not take a position on the difficult question of the borderline between forgery and agency arising through estoppel. This question must be decided by the courts.

2 Regulation of formal requirements

Note: This section has been formulated with three alternative models for implementing the fundamental equal status of digital and paper-based communication in relation to formal requirements for existence in writing and signature. The intention is, on the basis on the hearing, to decide which model should be incorporated in the final Bill.

As described under section A, there are a number of formal requirements that cannot directly, or may not even in the long term, be fulfilled by digital communication.

In practice, framework legislation aiming to achieve an equal status of digital communication and paper-based communication in areas with formal requirements can either be implemented via an exception or an inclusion model.

Under the exception model, digital messages with an authorized digital signature are basically put on an equal footing with paper-based communication in relation to formal requirements for existence in writing and signature. The exception model gives authority - temporarily or permanently - via Executive Orders to except Acts, Executive Orders or individual provisions therein which contain requirements for existence in writing or signature. The exception model will not enter into force until 1 January 2001 in order to give authorities time to go through laws, ensuring that all statutory requirements have been considered, that any amendments are in place, or that the necessary statutory requirements have been excepted.

Under the inclusion model, the Bill gives authority in each legal area to lay down administratively to what extent and in what way digital communication will be able to meet requirements for signature and existence in writing. A time schedule is set up for the Government's examination of laws etc. to ensure that amendment of rules in the relevant areas can be implemented as early as possible.

The difference between the two models is their significance as a political signal to the business community and consumers. While the starting point of the exception model is an equal status, the inclusion model is based on the assumption that each individual statutory requirement has to be expressly included. Another point is that the exception model will put greater pressure on individual Ministries with regard to arranging the

necessary amendments. But at the same time the model - especially if the timescale is too tight - may lead to massive exceptions, a situation which will not be desirable.

When the question was reviewed during the initial debate in the Folketing, a model combining the inclusion and exception models was proposed. Under this model, it should be possible, until the exception model comes into force, to lay down administratively to what extent and in what way digital communication can satisfy requirements for signature and existence in writing. Executive Orders issued before introduction of the exception model will be repealed when this model comes into force. This makes it possible, already from the commencement of the Act, to take steps to introduce practical equality.

Irrespective of the choice of a regulation model, the Government will take the initiative for a review of all legislation in order to clarify what statutory requirements for existence in writing and signature are in existence today. In the case of statutory requirements which cannot be satisfied today by digital communication, but where it should be possible to satisfy such statutory requirements, the Government will lay down a timescale specifying when it will be possible to use digital communication.

3. Duty of public authorities to use digital communication

The Bill lays down a requirement for public authorities to be able to communicate digitally with citizens who wish so, also in matters where some form of binding response is required from the citizen. The duty will not become effective until further decisions have been made by the Minister of Research and Information Technology and not earlier than 1 January 2001.

Such duty has practical as well as legal consequences. A practical consequence is that the authority must make communication lines available to the citizen and get the necessary equipment to enable communication with citizens who wish so.

The legal aspect is that an authority cannot reject a digital message from a citizen merely because the message is in digital form.

a. Document formats

While a paper document is immediately available, there is not one common standard today for representing digital documents. Digital documents may be represented in a great number of ways, as pure text, as a word processing document, in e-mail format etc. As a consequence, the use of digital technology implies the uncertainty that it cannot always be assumed that an addressee will be able to read a digital message since the technology does not yet ensure full compatibility between all systems, or

even within the same system. In connection with digital communication it is therefore essential that the sender of a digital document should use a document format that the addressee is able to read.

The problems associated with document formats are closely bound up with the questions of contract law as to when a message may be regarded as having reached the addressee, respectively been brought to his notice. The Bill has chosen not to take a position on this issue since it would appear to be more desirable to leave legal developments in this regard to the courts, as has been the case for current interpretation of the concepts of "having reached" and "having come to the notice of" in relation to paper-borne communication.

It must be a basic principle that in connection with the transmission of digital documents, generally recognized standards should be used. On the other hand, the addressee, if receiving an illegible message, must notify the sender of this.

The issues of contract law as to when a message "has reached", respectively "come to the notice of", have not been regulated specifically by the Bill. Is there a need for regulation, for example in connection with a regulation of e-mail addresses with special legal effects, and if so, what should be the content of such regulation?

However, in relation to the duty of the public sector to be able to send and receive digital messages under section 17 of the Bill, it has been considered desirable to give the Minister of Research and Information Technology authority to lay down more detailed rules for technical requirements for communication to and from public authorities and institutions. By laying down detailed requirements for this, transparency will be ensured for the citizen communicating with public authorities as well as definition of the duty of public authorities and institutions to use digital communication.

D. International developments

Establishment of a framework for digital communication is not an isolated Danish phenomenon. To a wide extent such systems must also be able to function globally if the business community and users are to derive full benefit of the facilities offered by the system.

It will therefore also be relevant to consider how far other countries have proceeded in regard to the regulation of digital signatures and what initiatives are in the pipeline in various international collaborative forums such as the EU, UN, WTO, OECD and G7.

In April 1997, the EU Commission issued a communication on electronic commerce, followed up in October 1997 by a communication on encryption and digital signatures.

The Commission calls on all member countries to initiate the necessary steps to ensure confidence in digital signature systems. In the Commission's view this implies that common requirements should be introduced for European certification authorities and key certificates, ensuring the possibility of mutual recognition of digital signatures, and it should also be ensured that secure digital signatures, in all areas where this is possible, will enjoy the same legal recognition as documents with handwritten signatures.

The Commission's communication was discussed at a Council meeting of Ministers of Telecommunications on 1 December 1997. The Council adopted a number of conclusions, asking the Commission to propose a Draft Directive on Digital Signatures as soon as possible. At the same time it was agreed to discuss relevant aspects of the Commission's communication in the Council of Ministers of Justice and Home Affairs.

The UN Commission on International Trade Law (UNCITRAL) adopted a model law in June 1996 on electronic commerce. The model law is based on the fundamental idea that electronic commerce requires that digital messages be put on an equal footing with paper messages, on condition that the functions served by paper are served equally well on a digital basis. This idea of functional equivalence is expressed in articles 5-7 of the model law which deal with requirements for existence in writing and signatures.

Article 5 of the model law indicates that information shall not be denied legal effect solely on the grounds that it is in the form of a data message. As for the requirement for information to be in writing, article 6 of the model law indicates that this requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference. As for signature requirements, it is stated that where the law requires a signature of a person, that requirement is met if a method is used to identify that person and to indicate that person's approval of the information contained in the message, and if that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated.

UNCITRAL has subsequently appointed a working group on digital signatures, which has been assigned the task of formulating guidelines for digital signatures and other electronic identification. The most recent meeting of the group was in Vienna on 19-30 January 1998.

In a number of countries initiatives are under way to promote digital communication. However, there is much uncertainty with regard to the specific content of future legislation in the individual countries on digital signatures etc.

In the United States a number of states have adopted legislation on digital signatures. Utah passed the first regular law on digital signatures, with regulation of certification authorities and giving legal effect to digital signatures. Since then a number of states have followed, with law initiatives differing widely in scope and content. However, at federal level it is still uncertain what initiatives the US Government will take with regard to digital signatures.

In Europe, Italy and Germany have adopted national legislation on electronic documents/contracts and digital signatures respectively. The German legislation is limited to cover only an authorization scheme for certification authorities, while the legal effects are not regulated.

In summary, the situation may be described as follows: there are a number of initiatives under way, both nationally and within the framework of international cooperative bodies. These initiatives have not yet assumed a character that may serve as a clear landmark indicating how international regulation in areas such as digital signatures will be in the last resort. It is the attitude of the EU Commission that the EU should make use of this situation and lead the way with regard to developing models for concrete legislation, thus being able to exert an active influence on future regulation.

With the present Bill, it may be possible for Denmark to derive a competitive advantage from being among the first in the market and being able to influence international solution models. On the other hand, it must be recognized that with an early Danish initiative in the area of digital communication, it may be necessary at a later date to carry out adjustments in the regulation when and if subsequent international initiatives are taken, for example a Draft Directive from the EU.

E. Administrative and financial consequences of the Act

1. Certification authorities

The function as a certification authority will be a free commercial activity within the framework set by the present Act. As a consequence, it is a prior condition that the activities of certification authorities will be financed via user charges.

Personnel costs must be expected in the form of a minor number of man-years in the National Telecom Agency for carrying out supervision, as well as personnel costs in connection with the appointment of an Appeals Board.

2. Consequences to public authorities

a. Review of all legislation

As described under section C(2), the Government will take the initiative to a review of all legislation in order to clarify what statutory requirements there are today for existence in writing and signatures. This review will be initiated no matter which model will ultimately be incorporated in the Bill.

The extent of this mapping project is difficult to estimate. A simple search in the Legal Information database indicates that there are about 4000 statutory requirements for existence in writing and another 1400 on signatures. If we include the underlying regulations in Executive Orders, the figure may approach some 10,000 statutory rules. All rules have to be reviewed, and for each individual provision it must be assessed whether digital communication may be used and what amendments of the statutory provision or Executive Order may possibly be needed.

The aim is for all Ministries to have completed this initial review of existing legislation before 1 May 1999. Depending on which equality model is incorporated in the final Bill, the individual Ministries must then, before 31 December 1999, have laid down specific timescales on how and when the necessary adjustments of Acts and Executive Orders will be completed, and have mapped the extent to which it will be necessary to introduce exceptions in case of an exception model. All amendments must have been made before 1 January 2001, when the principal rule of the Act is planned to come into force in case the exception model is chosen.

b. Duty of public authorities and institutions to communicate digitally

As for the duty of public authorities to communicate digitally with citizens who wish so, it is assumed that this duty will become effective from 1 January 2001 at the earliest and the Minister of Research and Information Technology, by way of an Executive Order, will lay down specifications for document formats that public authorities must be able to handle.

This duty may be met by setting up a central unit within the authority or institution for receiving and transmitting digital communication. For municipal administrations, the requirement may thus be met by setting up a communication facility in the mayor's secretarial office.

By the year 2001, public authorities and institutions should be able to communicate electronically with the surrounding world based on current standards. It is assumed that in using the authority of the Bill, the Ministry of Research and Information Technology will only refer to general and accepted standards.

In so far as authorities choose the minimum solution (one point of reception for each public authority/institution etc.), the Bill will only involve modest costs, which will be amply compensated for after an initial phase by the savings to be derived by using digital communication.

3. Commercial consequences of the Act

The Act should be seen in the context of the Government's national EDI action plan "Electronic Commerce in Denmark" (Ministry of Research and Information Technology, November 1996), where the Bill on Digital Signature is incorporated as a separate initiative capable of solving a number of legal and practical problems in using EDI.

Access to electronic communication based on common standards is expected to give added profits in individual companies due to rationalization and also to increase the competitiveness of companies via improved facilities for electronic interaction with other companies. Likewise it may be expected that the administrative burdens on companies will be eased because it will be possible for them to report information to public authorities electronically.

Legislation on digital signatures is being prepared in a number of other countries, and it must be assumed to improve the competitiveness of Danish trade and industry that Denmark is ensured legal clarification of these issues at an early stage.

4. Environmental consequences

Successively as the Bill becomes effective, it will involve clear benefits to the environment, partly because of lower resource requirements for transport of messages and partly because of savings in paper consumption. The Bill has no appreciable negative consequences to the environment.

5. Year 2000 consequences

(Will depend on replies to the hearing)

F. Hearing

This Draft Bill has been circulated for hearing to all Ministries as well as a number of relevant organizations etc.

Comments on the Individual Provisions of the Bill

Section 1:

The purpose of the Bill is to promote the secure and efficient utilization of digital communication. This will make it possible for society to derive clear benefits in the form of cheap, quick, flexible and environment friendly exchange of information, for example in terms of communication with public authorities and contracting between private individuals and companies etc.

The Bill therefore lays down a number of minimum requirements for certification authorities, authorized key certificates and for authorized digital signatures. The Bill embodies two alternatives for authorizations with different security levels.

A certification authority may obtain authorization to issue authorized key certificates, and the authority will then guarantee security in connection with the issue of the key certificate itself. Furthermore, a certification authority may obtain authorization to issue key certificates for authorized digital signatures. In these situations the certification authority will guarantee security in connection with the issue of the key certificate as well as the systems used for giving the authorized digital signature.

In view of the minimum requirements for security, it must be expected that the courts, in areas where there are no statutory requirements for signature and existence in writing, will basically recognize digital signatures which meet the minimum requirements of the law as secure. In addition, authorized digital signatures may be used in areas where the law requires existence in writing or signature, see section 6A/B/C of the Bill.

If a digital signature where the associated key certificate is authorized is used, there will only be a guarantee that the authorized key certificate has been issued under authorized conditions. Unlike authorized digital signatures, there will not be the same prior assumption that the security of the systems used for giving the digital signature is sufficient, and it will thus depend on concrete production of evidence whether such digital signatures may serve as a basis for legally binding transactions. Digital signatures where the associated key certificate is authorized will not be applicable in areas where the law stipulates existence in writing or signature, see section 6A/B/C of the Bill.

It is not intended to preclude the establishment of certification authorities or provision of digital signatures with associated key certificates that do not meet the stipulated minimum requirements for authorized key certificates and authorized digital signatures, nor does the Bill prevent the development of a market for digital signatures with a security level higher than the minimum requirements of the law.

If digital signatures are used outside the authorization scheme, they will rely on the production of concrete evidence, partly on whether the key certificate was issued under sufficiently secure conditions and partly on whether the systems for giving the digital signature are sufficiently secure.

The Bill lays down a number of minimum requirements regarding the liability of certification authorities to pay compensation as well as other obligations of certification authorities. The rules apply to certification authorities both with and without authorization.

Section 2:

The proposed provision aims to define digital signature according to this Bill in relation to other forms of digital identification, including systems for electronic identification that do not involve a certification authority. Thus it is established that digital signatures under the present Bill must be generated by means of an asymmetric encryption system and that the public signature key must be registered by a certification authority.

This definition does not preclude agreements to the effect that the Act should be applied in areas where it would otherwise not be used automatically, for instance in systems that do not employ certification authorities. Nor is it intended that the Bill should interfere with existing contractual relationships between private parties.

The Bill does not intend to exclude digital identification methods and securing of evidence in digital messages other than those employing asymmetric encryption and registration of the public key by a certification authority. It will be a matter for the courts to take a concrete decision on digital signatures given in other ways.

The Bill will apply to authorized certification authorities as well as certification authorities without authorization.

Section 3:

The proposed provision aims to delimit the Bill on Digital Signature etc. in relation the Act on Payment Cards.

The Bill on Digital Signature etc. regulates a technique which corresponds in many respects to the technique used in payment systems, for example the "Dancard" system. Both for digital signatures and payment transactions via Dancards, encryption techniques are used for secure communication.

In the long term, there will probably be instances in which systems for digital signature and for carrying out payment transactions will be available, in many cases, on one and the same medium so that the user may carry out several types of transaction by using the same card. Here it will be essential to be able to distinguish the various functions so that use of the same card for signature and payment does not give rise to any doubt to the customer. It will be important for a user, for instance, to be able to distinguish when entering into an agreement with subsequent payment. Has a digital signature been given in this situation, or has the user already, in reality, completed a payment transaction?

Regulation of payment systems differs in several respects from the present Bill, and it is therefore essential to be able to separate payment transactions and payments transfer as identified in section 1 of the Act on Payment Cards from digital signatures. The difference between systems for digital signature and payment systems will typically be that some form of guarantee is associated with a payment system, the card issuer guaranteeing a certain amount in relation to the payee, while a digital signature merely serves to identify the keyholder. The difference between regulation of digital signatures and payment systems appears, among other things, from the liability rules, see comments on section 7.

It will therefore be essential for systems for payment and systems for digital signature to be separated logically to make it clear to the user when he is signing and when he is carrying out a payment transaction.

Consequently the present provision stipulates that integrated systems that may be used both for giving digital signatures and for payments transfer must be arranged by the service provider in such a manner that it will be possible for the user in connection with each individual transaction to distinguish clearly between the two functions.

For example, it might be possible to allocate different PIN codes to the two systems so that the user would always be aware which type of transaction is being made. In this area it may be necessary to have supplementary rules for consumer protection, as commercial and consumer interests do not seem to be the same.

The provision does not intend to regulate software manufacturers, but is aimed at certification authorities in connection with the approval of systems that may be used for generating authorized digital signatures. A certification authority recommending systems to its users must therefore ensure that the systems meet the requirements of this provision.

Section 4:

The aim of this provision is to define a number of central concepts in the Bill.

Subsection (1):

The provision defines a key pair for digital signature. The concept "key pair" is not included in the wording of the Act as such, but the interrelation between the private and the publicly accessible signature keys of the key pair is crucial to understanding the technique underlying digital signatures, see General Comments, section B.

Subsection (4):

The definition of a certification authority is essential because the Bill stipulates a number of requirements for the certification authority's duty to give information and the extent of its reliability. It is not intended through this provision to include all issuers of key certificates, e.g. key certificates solely used for admittance control etc. The Bill solely refers to key certificates used in connection with the affixing of digital signatures.

Subsection (5):

A keyholder as defined in subsection (5) may both be a natural and a legal person. In the long term it is conceivable that the technique underlying digital signatures will be used for giving legal persons the capability of undertaking obligations as such by means of digital signatures. However, this capability falls outside the scope of this Bill.

To legal persons the legal effects of a digital signature according to this Bill may be compared with using a firm's letter paper, as the digital signature will merely provide evidence that the message originates from the legal person in question, but not necessarily that the legal person will be liable for the contents of the message. If the company wants to attest to the contents of a message, the message must be signed by the natural person(s) who are empowered to sign for the company.

Subsection (6):

Time stamping is a declaration indicating that specific digital information existed at a specific time.

In practice, time stamping may appear, for example, as a digital signature on a certain amount of digital information including an indication of time.

Time stamping may be used to provide documentation to ensure that a given message existed at a specific time or to "refresh" the security of a digital signature which is about to expire, see General Comments, section C(1).

Under section 14 of the Bill, authority has been given to require authorized certification authorities to ensure users access to time stamping, thus enhancing the security of evidence.

Section 5:

This provision lays down definitions of authorized certification authorities, authorized key certificates and key certificates for authorized digital signatures.

Sections 6A-C:

Note: At present the Bill contains a description of three alternative models for implementing the fundamental equal status of digital and paper-based communication in relation to formal requirements for existence in writing and signature. The intention is, on the basis of the hearing, to decide which model should be incorporated in the final Bill.

The intention of the Bill is to create a foundation which will ensure that a digital signature may be just as good as a handwritten signature, and that it will consequently be possible to use digital messages with digital signatures in all areas where paper and handwritten signatures are used today.

Basically, the signature itself does not pose any problems. In Danish law it is a traditional starting point that there is no requirement as to how contracts should be made. A contract remains valid even if it is not written on paper with a signature. If you nod your assent or accept an agreement verbally, it is just as binding as if written on paper.

The rules of the Bill on digital signature will provide a high degree of security for the identity of the sender of a message and for the validity of its contents. However, it is not possible to bind the courts to accept a digital signature since this would be contrary to the principle of freedom to assess evidence. But in view of the legal basis for digital signatures, it must be expected that a digital signature will have considerable evidential weight.

On the other hand, the starting point that a digital signature and a handwritten signature are equally good may give rise to problems in areas where Acts or Executive Orders include requirements for signature or existence in writing.

In connection with formal requirements, it will primarily be a condition that the digital message should be legible, see General Comments on the Bill, para. B(c). Secondly, it will also be a requirement that the digital message should be available in a permanent or lasting form so that it may subsequently be recreated in the same manner as is used in the case of e-mail or diskette files. But a requirement for existence in writing will not have been met merely because a call is made from a digital telephone.

In addition, a number of various considerations may be underlying a requirement for existence in writing or signature, according to the needs to be fulfilled by the requirements. In many cases a formal requirement may very well be met via a digital document provided with a digital signature. For example, the requirement may only indicate the wish to have security of the identity of the sender of a document or security of the contents of the document.

In other cases the requirement for existence in writing will involve a prior condition for communication on paper, e.g. specific forms or blanks to be filled in, conferring a specific legal status on the person(s) possessing them. This is the case for documents such as cheques and bills, passports and driving licences, which are all document types that cannot immediately be digitized. At any rate, there is no sense in making digital money or cheques without protecting against copying.

In the consumer area there may be special protective considerations behind statutory requirements for existence in writing or signature, e.g. ensuring, via a concrete process of written signature, that the consumer will be made aware of the consequences of specific acts, or that a concrete set of contract terms is handed to the consumer.

Certain conditions of an administrative, practical or financial nature will mean that the law needs to be adjusted before digital messages will be able to replace such paper-based documents. This applies, for instance, to the rules on submitting written tenders in response to public invitations to tender, where it may be required that envelopes should be opened at the same time. These rules may be adapted to the electronic universe, but will call for an amendment of the law.

Furthermore, there may be international agreements or EU legislative acts which prevent Danish legislation for the purpose of giving an equal status to digital and paper-based communication in relation to formal requirements. An example of such legislation is the Credit Agreement Act, which is based on a EU Directive on consumer credit. The Act contains a requirement for existence in writing for all consumer credit agreements, and in the last resort it will be for the EC Court of Justice to decide whether this requirement can be met by digital communication.

Finally, there may be formal requirements in areas where - at any rate within the foreseeable future - there is no sense in using digital communication. This applies to those areas in which formal requirements are bound up with the wish to be able to identify an original document. Here it will typically be necessary to introduce extensive technical and organizational changes before digital communication can be used. Such techniques are available, but the question is outside the scope of this Bill.

Section 6A:

According to the exception model, digital messages with digital signatures are basically put on an equal footing with paper-based documents with handwritten signatures in relation to formal requirements for existence in writing and signature. The exception model gives authority - temporarily or permanently - via Executive Orders, to exempt specific Acts, Executive Orders or individual provisions therein which contain requirements for existence in writing or signature.

The equality principle is not only linked to cases in which the wording of an Act expressly stipulates existence in writing or signature, but also to situations in which this requirement is "implied". This allows for such verbal passages in the law as do not expressly require existence in writing or signature. For example, there may be a requirement to the effect that a form has to be filled in or a declaration has to be submitted.

Both in case of a requirement for existence in writing and a requirement for signature, a digital signature has to be affixed to a digital message in order to meet the requirement. In those cases where existence in writing does not involve a requirement for signature as well, it might be alleged that it would be sufficient to send a digital message without a digital signature. However, the digital signature does not only add a signature, but it also ensures that the document has not been altered after it was originated. So this quality gives a digital message the same quality as possessed by a paper message, in contrast to a verbal message: that subsequently there is security for the contents of the message, because the document cannot be altered without the alteration being traceable.

It has been proposed that the exception model should take effect from 1 January 2001 so that authorities will have time to review legislation to ensure that all statutory requirements have been considered and that any amendments are in place, or that the necessary statutory requirements have been excepted if necessary.

Subsection (2):

The general principle of equality as indicated in subsection (1) cannot be implemented directly in all areas. Certain requirements for existence in writing and signature must be excepted temporarily or permanently from the general equality rule of subsection (1).

To avoid any doubt as to which provisions with requirements for existence in writing or signature should be excepted from the general equality principle of the Act according to subsection (3), it is proposed to issue Executive Orders specifying the provisions where digital communication will not be able to satisfy formal requirements. The requirements for existence in writing and signature that may be departed from by Executive Order may appear from Acts as well as Executive Orders.

In relation to the requirements for existence in writing and signature included in the Executive Order on exceptions, it is intended to lay down an action plan for implementing the equality to the extent that the exception is of a temporary character.

Section 6B:

According to the inclusion model, the Bill provides authority in each legal area to lay down administratively to what extent and in what way digital communication may satisfy the requirement for signature and existence in writing.

It is planned to set up a time schedule for the Government's review of legislation etc. to make it possible for amendment of rules in the relevant areas to be implemented as early as possible.

Section 6C:

This model combines the proposed provisions of sections 6A and 6B. Section 5A (the exception model) will be the solution in the long term, while section 6B (the inclusion model) will apply in the transitional phase. This model will thus solve the problem that if the exception model is chosen with a late implementation date, there will in reality be a longer period in which authorities that wish to introduce practical equality between digital and paper-based communication would have to introduce amendments to Acts.

Under this model, authorities that wish to start digital communication in the near future may use the authority to lay down rules about this through Executive Orders. When the exception model enters into force, these Executive Orders will be repealed, see the proposed section 25a.

Section 7:

The aim of this provision is to lay down rules for barring of a key certificate.

Barring of a key certificate should be made in situations where a keyholder loses control of his private signature key, for example if an unauthorized third party gets access to the keyholder's chipcard or PC where the private signature key is stored.

In such situations the keyholder should immediately ask the certification authority to bar the key certificate to avoid misuse. If the keyholder fails to request barring in cases where the keyholder knows or has reason to believe that an unauthorized third party has access to his private signature key, the keyholder may incur liability in relation to an addressee in good faith, see comments on section 11. How the keyholder should request the certification authority to bar his digital signature will depend on the guidelines of the individual certification authority.

The Bill stipulates that barring will take effect from the moment when this has been announced by the certification authority. However, there will be a period from the time when the barring message arrives at the certification authority till the certification authority announces the barring. The question is who should bear any losses sustained by addressees during that period. It is proposed in this provision that the keyholder should bear the risk of claims for compensation from addressees in good faith since the reason for barring will typically be due to conditions ascribable to the originator.

Under section 14, more detailed rules can be laid down for publication of notices for certification authorities that issue authorized key certificates.

Subsection (2):

This provision aims to regulate the effect of a key certificate being barred. The addressee of a digital signature where the associated key certificate is barred cannot base any right on the digital message in question unless the addressee can establish that the signature was given before the time of barring.

The decision as to whether a specific digital signature was given before or after the barring may, as described in General Comments under section C(1) and in the comments on section 3(8), involve problems in a few situations since it does not appear from the signature itself when it was given.

The time of barring will be the only factual and demonstrable indication of time.

When the addressee observes in connection with the verification of a digital signature that the key certificate is barred, he should request the keyholder to confirm or disconfirm the signature in other ways, for instance by asking for a digital signature

where the associated key certificate is not barred or by requesting some other form of acknowledgment from the sender, e.g. a paper message with a signature.

However, if the keyholder denies having given the signature, it will for the addressee to establish that the signature was given before the barring.

In some situations the addressee will have reason to believe, in connection with the verification, that the signature was given before barring of the key certificate. It is conceivable, for example, that a user receives an e-mail on a Thursday, but does not have the occasion to open it until Saturday. The e-mail contains a message with a digital signature. When the user seeks verification of the signature in the database, it turns out that the key certificate was barred on Friday.

In this example the signature was given before the time of barring, but an evidence problem may arise if the originator denies having signed the document in question and if the addressee is not able to establish that the signature was given before the time of barring.

It may be possible to produce technical evidence to show that the message was signed or sent from the originator before the time of barring. For example, log files held by the sender, any information carriers used or the addressee may indicate that the document was filed before the time of barring.

However, the starting point must be that the party who wants to rely on the content of the document must establish that the digital signature was given before the barring.

As described under the comments on section 3(8), the addressee may enhance the security of evidence in relation to the barring question by letting an independent third party affix a time stamp to the message and/or signature.

The certification authority's absolute liability will cease when a key certificate is barred, see section 11(4).

Section 8:

This provision regulates the special consideration that a digital signature affixed to a digital message will gradually become obsolete as the technique allowing the code to be broken gets faster and more sophisticated. In a few years' time the elements that constitute a secure digital signature today will no longer protect against forgery etc.

The obsolescence issue reflects a basic difference between digital and handwritten signatures. When using digital signatures, users should carefully consider how their

digital documents will be stored. Documents that may become important beyond the expiry period of the involved digital signatures must be stored with care.

A key certificate will typically contain an expiry date. The Bill requires authorized key certificates to specify an expiry date, see subsection (2).

The Bill proposes that the consequence of a key certificate expiring will be that addressees cannot base any right on the digital signature unless it is established that the signature was given before expiry of the key certificate, and that the digital message was supplemented before expiry of the key certificate with a digital signature where the key certificate has not expired.

When a key certificate has expired, two requirements must thus be fulfilled:

In the first place, it must be established that the digital signature was given before expiry of the key certificate. See comments on section 7 on similar conditions in connection with barring.

Secondly, a digital signature where the key certificate has not expired must have been affixed to the digital message before expiry of the key certificate. In other words, the digital message must remain signed at all times with a "fresh" key so as to ensure that the integrity of the document will be preserved. There is no need for the same persons to sign again. It is only necessary to lock the document with a new signature key so that no one can tamper with it. Such solution may be realized by affixing one's own digital signature to the document or to cause a time stamp to be affixed, see comments on section 3(8). But to secure proof that "refreshment" was made before expiry of the signature, it will be necessary in all cases to have a time stamp.

Reference is made to the question box within the text of the Bill directly after section 9.

An example of the expiry process: If you have made an agreement with a landlord to rent a house for ten years, and the landlord's digital signature expires in four years, the digital message must be "refreshed" before expiry of the four years. You may either choose to use your own digital signature to lock the document, or you may apply to the certification authority and have a time stamp put on the contract, the integrity of which will then be secured for a further period. If you use your own digital signature, it will be desirable to use time stamping anyway, so that you will be able to prove when you affixed your digital signature.

When a key certificate has expired, the certification authority's absolute liability will cease, see section 11(4).

Section 9:

This provision enables the certification authority to impose restrictions on the use of the digital signature in the key certificate. As to the grounds for using restrictions in the key certificate, see General Comments on the Bill, section C(1).

Subsection (2):

This provision gives authority for the Minister of Research and Information Technology to lay down specific categories of usage restrictions on authorized digital signatures.

If certification authorities have free access to determine the application area, this might involve unnecessary administration in connection with the verification of digital signatures because it will be necessary to go through the various specifically framed restrictions of individual key certificates to clarify whether a user may base any right on a specific application.

It is therefore proposed to lay down a limited number of restrictions on usage. Such categories must be determined in cooperation between the industry and user representatives and may include the following general categories:

- Communication with public authorities
- Family law transactions
- Electronic commerce
- Buying and selling of real property

Subsection (3):

If a digital message with a digital signature falls outside the application area, no right can be based on the digital message in question. At the same time the certification authority's absolute liability will cease, see section 11(4).

See the question box within the text of the Bill directly after section 9.

Section 10:

The aim of this provision is to enable the addressee to get information on any barring, expiry or restrictions on the application area in connection with the verification of a digital signature.

The Bill proposes that the certification authority should give information on these matters on request. As for expiry and restrictions on the application area, this will typically appear from the key certificate, and the requirement according to section 10 may therefore be met by the certification authority giving potential addressees of digital signatures access to key certificates issued.

As far as barring is concerned, the Bill does not stipulate how this information should be made available by certification authorities without authorization. For certification authorities with authorization, authority is provided in section 14(5) to regulate this matter.

Section 11:

Despite an authorization scheme being introduced for the purpose of ensuring the reliability and integrity of certification authorities, and hence digital signatures, faults may naturally occur as in all systems. These faults may involve a loss partly to the keyholder and partly to the other party who is acting in reliance on the signature.

For example, there might have been a fault in connection with the issue of the key certificate because the certification authority has not observed the prescribed regulations for securing the keyholder's identity or for the technical design of key certificates. There may also be cases in which the signature keys do no live up to prescribed security regulations. Furthermore there may be defects on the diskette or chipcard on which the signature key is stored. Finally there may be errors in the certification authority's information about the validity, expiry date etc. of the individual key certificates.

Subsection (1):

A certification authority is liable to the keyholder as well as addressees of digital signatures for any loss due to failure of the certification authority to observe the regulations that the certification authority has adopted for its own activities in its certification practice, see also comments on subsections (3) and (4).

The liability for such faults is absolute, i.e. the certification authority must also compensate for loss due to accidental faults.

Subsection (2):

A certification authority issuing authorized key certificates is liable to pay compensation as described in subsection (1) and furthermore the authority is liable on an absolute basis for loss due to failure to comply with the minimum requirements laid down for authorized key certificates pursuant to the Bill. This applies to a number of security procedures regarding identification of users, generating keys, issuance and handling, including any barring, of key certificates.

Subsection (3):

A certification authority issuing key certificates for authorized digital signature is also liable to ensure that the security of the systems employed by the user for giving digital signatures complies with the minimum security requirements of the Bill, see section 14(6).

Based on the minimum requirements of the Bill, the certification authority may prescribe what systems the user may employ for digital signature and how long the certification authority will guarantee the key certificate. If these systems cannot live up to the stipulated minimum requirements, the certification authority must compensate for any loss arising out of this, see section 11(3).

In those situations where the user is co-responsible for the security of the digital signature, it will be possible for the certification authority to adduce evidence to show that the fault was due to the user's negligence. If the certification authority establishes that a loss is due to circumstances under the user's responsibility and that it may be ascribed to the keyholder's negligence, the certification authority's liability in relation to the keyholder may be reduced or cease, and the certification authority may have recourse against the keyholder for any compensation paid to addressees.

The areas in which the user is co-responsible are notably concerned with the secrecy of the private signature key. In case the keyholder, through culpable conduct, makes it possible for a third party to get access to the private signature key, the certification authority's liability in relation to the keyholder will be reduced or cease, while any claims of addressees may pass wholly or partly to the keyholder.

If, for example, the keyholder fails to protect his signature key with a PIN code or gives the PIN code to a third party, any liability to pay compensation should rest with the keyholder. This should also apply in case the keyholder is using his signature key together with systems other than those approved by the certification authority.

To the extent that it has been prescribed to the keyholder what systems he may use for giving digital signatures, the keyholder is under an obligation to use these. If the keyholder uses other systems and this may be established by the certification authority, the keyholder will have to bear any loss arising, wholly or partly.

Subsection (4):

The certification authority's absolute liability under section 11(1)-(3) will cease to the extent that a key certificate is barred or has expired, or to the extent that a digital message with a digital signature falls outside the application area specified in the associated key certificate.

Subsection (5):

In those situations where all regulations have been observed by the certification authority, the liability to pay compensation will be decided by the general compensation rules of Danish law.

Subsection (6):

This provision aims to regulate those circumstances in which a digital signature has been given through forgery. The question of liability and compensation in situations involving forgery must be decided according to the general rules of Danish law for liability and compensation in case of forgery.

The Act on Payment Cards imposes liability to a certain extent on the bank, credit card company or retail chain that has issued a payment card also in a situation where the card has not been barred on the part of the cardholder, i.e. a situation where a thief has come into possession of both a Dancard and the PIN code.

It is natural for the Act on Payment Cards to impose such extended liability on banks, credit card companies, retail chains etc. It is the professional task of these companies to offer payments transfer, and in this connection they derive a clear financial and administrative advantage from the existence of payment card systems. Another aspect is that the companies, by virtue of their general role of arranging payments, have the option of charging this loss to payees, who will then bear the loss jointly and severally.

That this regulation model is feasible in relation to payment cards is also due to the fact that it is always possible to determine in advance the exact amounts for which the card issuer may become liable, and that it is possible to limit this potential liability via drawing rules etc. However, a digital signature may be linked to any transaction, which makes the potential loss unknown and much more uncertain. If such extended liability were imposed on certification authorities, it would therefore put severe restraint on the establishment of these.

The fact that there are different liability rules for the use of payment systems and systems for digital signature necessitates a clear distinction between these two areas. Thus it must be ensured that it is clear to the consumer when a payment transaction, respectively a digital signature, is being dealt with, see comments on section 3.

Section 12:

The proposed provision aims to ensure that a certification authority gives the necessary information to potential users. The provision is applicable to certification authorities operating on the basis of an authorization as well as non-authorized certification authorities.

The provision requires the certification authority to give information about the authority's certification practice and general business terms.

The Bill stipulates that this information, as a minimum, should include a description of the certification authority's procedures for issuing key certificates, including the certification authority's rules for verifying the keyholder's identity, the certification authority's internal security procedures etc. Such information will typically come under a certification practice, but since no fixed practice for the content of such declarations may yet be said to exist, it has been found desirable to lay down these minimum requirements in the text of the Bill.

Section 13:

This provision regulates the protection of personal data in connection with an authorized certification authority's issue of key certificates for authorized digital signatures.

The provision applies both to authorized and non-authorized certification authorities. It refers to a Bill for an Act on Processing of Personal Data etc., expected to be passed by the 1998/99 session of the Folketing, based on EU Directive 95/46.

The provision aims to prevent certification authorities from using personal data obtained in connection with the issue of key certificates for other purposes, e.g. marketing activities.

Section 14:

To build up the necessary security and confidence for giving digital signatures based on certification authorities, it is proposed that this activity be based on the basis of public authorization. This will be in the form of private enterprises which may seek authorization through the Minister of Research and Information Technology.

Although it is basically assumed that certification authorities should be established within a private framework, it may also be relevant to set up publicly owned certification authorities in connection with institutions such as the Central Business Register (CVR) and the Civil Registration System (CPR). These two registers have special qualifications which enable them to give the secure business or personal identification that forms the basis for the activities of certification authorities.

The access to authorization is optional for certification authorities, and it is not proposed to stipulate that the activities of certification authorities may only be carried on under an authorization. Such requirement would constitute a barrier to foreign certification authorities' access to the Danish market, which must be considered as contrary to Denmark's commitments under EU law. At the same time it must be expected that a market will arise for security-related services based on the issue of key certificates etc. which will not comply with the requirements of the Act.

A certification authority may apply for authorization for the purpose of issuing authorized key certificates or for the purpose of issuing key certificates for authorized digital signatures.

The two authorization models represent two different security levels. While the certification authority issuing authorized key certificates is solely guaranteeing security on and in connection with the key certificate, the certification authority issuing key certificates for authorized digital signatures is also guaranteeing security in the computer system and the signature key employed by the keyholder.

The two authorization models thus differ only in that the certification authority issuing key certificates for authorized digital signatures undertakes a guarantee to addressees for the software that the originator is using for generating keys and affixing authorized digital signatures.

As to the difference between the legal effect of using an authorized key certificate and a key certificate, reference is made to General Comments, section C(1).

More detailed conditions for obtaining authorizations will be laid down by Executive Order, see subsection (3). The reason why it is not proposed to lay down requirements in this respect in the Act itself is that international growth is expected in the market, and it will be desirable for Danish authorization requirements to be able to reflect international developments on a current basis.

To obtain the Danish State's authorization, certification authorities must be under Danish jurisdiction since the public supervision associated with the authorization may only be exercised within the territory of the Danish State.

Subsection (4):

Requirements for the company under section 14(3) may include capital basis, insurance conditions and security routines.

Subsection (5):

Under this subsection, the Minister of Research and Information Technology is to lay down more specific rules for the activities mentioned under nos. 1-5, to be carried out by a certification authority when issuing key certificates for authorized digital signatures.

No. 1:

The linking between a natural or legal person and the person's signature key is crucial to the security of digital signatures. If a certification authority, by mistake, issues a key certificate indicating that Mr. A "is" Mr. B, this will mean that Mr. A will be able to pose as Mr. B. Consequently it is one of the essential questions in designing systems for digital signature to ensure that a person will not have issued a key certificate under false identity.

It will probably be required that the user should appear personally at some stage in the registration process, either before the certification authority or before an authority appointed by the certification authority (e.g. a post office, a bank or the national registration office, which may act as local registration authorities), establishing his identity by means of a valid ID card with a photo, e.g. a passport or driving licence. This requirement is to minimize the risk of faults in the key certificate.

In addition, it must be considered whether there should be a requirement for verification of the identity via the civil registration system (CPR) as regards persons with a residence permit in Denmark, or the central business register (CVR) as regards businesses registered there. Based on the user's CPR or CVR number, the certification authority will be able to verify information about the user's identity such as this appears from the identification papers shown. In this manner the certification authority will be sure that the person in question is a person actually existing (not a made-up existence) and that the person is not registered as deceased or disappeared.

The certification authority will probably be allowed to leave the practical identification of keyholders to authorities or enterprises (e.g. national registration offices, banks or post offices), but the responsibility for observance of procedures will lie with the certification authority, see comments on section 11.

No. 2:

The authorized certification authority will issue a key certificate to the user. The certification authority must prepare the necessary security procedures to ensure that key certificates issued contain correct factual information about the user's identity and the associated signature key.

In connection with the issue, the certification authority will be required to work out procedures to ensure that key certificates are unique, and that key certificates are not issued to different persons with the same key pair. The certification authority may leave the practical issue of key certificates to other authorities or enterprises, but the responsibility for observance of procedures will lie with the certification authority.

Minimum requirements for the content of key certificates are regulated in section 15 of the Bill.

No. 3:

The certification authority must set up and maintain a database of issued key certificates for authorized digital signature.

It will be a requirement that the database should be available electronically to potential addressees of digital signatures. This means that a database in a system where there is only an addressee (e.g. certain systems for homebanking) should only be available to this addressee.

It will be required that the database should be maintained for at least 10 years after expiry or barring of the individual key certificate because it may also be necessary after this period to be able to check whether a digital signature given earlier has been brought about by the indicated originator's private signature key, e.g. in case of a dispute over an old tenancy agreement existing in digital form, and where it is to be established whether it was signed by an earlier landlord. It is the certification authority's responsibility to ensure that such key certificates can be made available.

No. 4:

Access to information on barring should be electronically available to potential addressees of digital signatures with the key certificate in question.

It may be relevant to lay down more detailed rules on how the certification authority should make information on barring available, but it will probably be sufficient to have a functional requirement to the effect that addressees of digital signatures, by means of a single reference with the certification authority, should be able to get the necessary information to verify the digital signature, i.e. all information as mentioned in section 10(1).

It will be a requirement, however, that the certification authority respond immediately to a request for barring, and the certification authority will be liable to pay compensation to the keyholder in case it fails to announce the barring immediately, see section 11.

No. 5:

In addition to the fundamental security service in the form of identification, the certification authority should also offer users access to time stamping of digital messages, see comments on section 3(8) of the Bill.

This provision may also be used to lay down more detailed rules on the time stamping process to ensure that this is sufficiently secure.

Subsection (6):

The certification authority is to ensure that the access to use authorized digital signatures as established hereunder fulfils the statutory requirements for authorized digital signatures.

This provision gives authority for the Minister of Research and Information Technology to lay down qualitative requirements for the products (software and hardware) as well as algorithms and signature keys to be used for giving authorized digital signatures.

Based on the requirements laid down by the Minister of Research and Information Technology, certification authorities issuing key certificates for authorized digital signatures may prescribe what products can be used for authorized digital signatures.

Certification authorities may choose to offer their own products for digital signatures. In these situations the requirements will form the basis for the products supplied by the certification authority for authorized digital signatures.

Products for digital signature will probably be supplied to a greater extent by software or hardware suppliers, for example as an integral part of the user's PC, incorporated in the PC operating system (e.g. Windows) or incorporated in the user's e-mail

program or Internet browser. In this case it will be the certification authority's job to assess and approve the range of products which, according to the stipulated requirements, may be used for authorized digital signatures.

The certification authority will incur liability if the software approved or supplied by the certification authority does not fulfil the minimum requirements of subsection (1).

Efforts will be made to formulate the stipulated requirements in such a manner that, on one hand, they are sufficiently concrete to determine if a given product complies with the requirements, while, on the other hand, they will preferably be kept in terms so general that the requirements will not become obsolete too early as a result of technical developments.

In the light of this, it is believed to be desirable, as a general rule, to draw up functional requirements for the products - possibly described via well-known examples - and to draw up more specific technical requirements in special areas only.

On one hand, the requirements for authorized digital signatures must be able to ensure a high quality. On the other, the requirements must necessarily reflect the current technological capabilities available in the market so that they can be met without imposing excessive costs on certification authorities or users. For example, it will probably be required in the longer term that private keys should be stored on chipcards or other hardware tokens. On commencement of the Act this may be too costly since chipcards and infrastructure for using these have not yet become generally available in the market.

At the present time, the following requirements may be foreseen:

- Algorithms
  Open and standardized algorithms must be used whose security is widely recognized, e.g. RSA, DSA, Diffie-Hellman.

- Key lengths
  The key lengths used in the system must give a security corresponding to RSA keys with a length of 1024 bits.

- Key generating
  The principles of key generating (e.g. choice of a random generator) must ensure generating of keys with a high level of security.

- Key storing
  The private signature key must be stored securely, e.g. on a chipcard, in other hardware or in software protected by password encrypting.

- Requirements for verification of digital signatures
  The product must be able, in a secure manner transparent to the user, to verify the validity of the key certificate and indicate the expiry date and any restrictions on the application area.
  The product must be able, in a simple (an preferably automatic) way, to check whether the key certificate is barred. The addressee must be informed clearly whether such checking has been made and what the result is.

- Requirements for transparency
  It must be clear to the sender what message is being signed and to the addressee on what message a given digital signature has been given.

Section 15:

This provision lays down a minimum level for the information to be included in an authorized key certificate.

No. 1

The unique identification of the keyholder is to protect against mistakes in key certificates. The unique identification may for example be the name plus an amount of additional information ensuring that there are no other individuals with the same identification data. Another possibility is an account number in a bank etc.

The most obvious solution for systems to be used universally is of course to use civil registry numbers (CPR) in the key certificate. With the CPR number in the key certificate, there will be a unique identification, at any rate for persons with a residence permit in Denmark, thus providing protection against mistaken identities. The use of CPR numbers will also mean easier administration for public authorities in connection with electronic processing of forms etc.

For added privacy, the CPR number might be shown as a hash value, i.e. in coded form, where only persons who already know the originator's CPR number will be able to verify the number by using a computer program. Persons who do not know the originator's CPR number in advance will only see a number of digits, which, however, will meet the requirement for uniqueness.

All the same, it has not been proposed to use CPR numbers in the key certificate itself, which is due to the fact that CPR numbers are limited to Denmark and that not all systems, for instance under public authorities, are necessarily using CPR numbers.

No. 2.

See comments on section 8.

No. 3.

It must appear from the key certificate that it has been issued by an authorized certification authority and whether the certificate in question and the underlying system for generating digital signatures comply with the requirements of the Bill for authorized digital signatures.

No. 4.

See comments on section 9 and General Comments, section C(1).

Section 16:

This provision aims to make it possible to recognize foreign certification authorities, key certificates and digital signatures that meet the requirements of the Bill for authorized digital signatures.

The use of digital communication and hence digital signatures is spreading to a wide extent across national borders. It must therefore be expected that we will soon have a situation in which there will be a need of recognizing foreign key certificates or deciding to what extent an addressee of a digital message provided with a digital signature may rely on the signature as being binding on the originator. It is therefore proposed that the Minister of Research and Information Technology should be empowered to lay down rules for meeting international agreements. An initiative may be expected from the EU Commission for EU law regulation, but in the long term there may also be agreements on an international basis, e.g. within the framework of the UN or WTO.

It is not yet clear how international agreements on recognition of digital signatures will be drawn up. It would be possible to have a recognition procedure at several levels. The most obvious solution would be for the national regulatory authorities of individual countries to form agreements on mutual recognition, but it is also conceivable that there will be a mutual recognition on certification authority level so that certification authorities recognize and guarantee each others' key certificates.

Section 17:

The proposed provision is to give public authorities and institutions governed by the Public Administration Act a duty to receive digital messages.

In this way it should be made possible for citizens and companies as early as possible to choose digital communication as an equal alternative to paper-based communication. In the long term a transition from paper-based to digital communication will involve very substantial savings to the community in terms of time and resources, and the public sector should therefore lead the way in realizing such savings.

In connection with the proposed "duty" to receive digital messages, there is both a practical side and a legal side. The practical side is that the authority has to establish the communications channels to the surrounding world that are necessary to allow digital information to be transmitted to the authority. On the introduction of the Bill, the Internet is the most frequently used form of communication, but developments within communications may very well produce other facilities which the authority will then have to make use of in order to meet the requirements of the law.

The legal side of the duty is that an authority actually receiving a legible message must also be regarded in a legal respect as the receiver of that message. "Reception" as dealt with in section 17 means that a digital message entering an authority's computer system is regarded as having reached that authority. The duty of a public authority to receive digital messages thus means that an authority cannot reject a digital message merely because the message is in digital form.

In view of the fact that such general duty to receive digital communication, as mentioned already, will involve practical preparations and a certain amount of costs, it is proposed that the duty should take effect from a date to be decided more specifically by the Minister of Research and Information Technology, and not earlier than 1 January 2001.

The duty to receive digital messages is general, which means that the authority may decide for itself how digital messages should actually be received by the authority and be distributed internally. Thus the authority may decide for itself whether it wants to receive digital messages at one point within the authority, where they are printed out and distributed in a paper-based form to the relevant recipient (or via internal e-mail), or whether the authority wants to establish several reception points for digital messages within the authority, for example to enable digital messages to be sent directly to individual employees. In the long term this may be expected to be the solution, but in a transitional phase it may be necessary for the individual authority to limit itself to one single reception point.

Definition of relevant areas within the public sector means that the Folketing and its institutions as well as the courts do not immediately come under the Bill, but it will depend on the result of the hearing whether these institutions should be included under the duty in section 17 all the same. Furthermore, a number of institutions established

on the basis of private law, e.g. self-governing types of schools such as business colleges and technical schools, are not included. Here, it has been found more correct to let the duty follow the categories referred to in the Public Administration Act so that institutions established on the basis of private law, but subject to the Public Administration Act, will also come under the Bill.

Subsection (2):

The authority will be used for defining what document formats public authorities should be able to handle.

Subsections (3) and (4):

Under subsection (1), public authorities are required to offer citizens a liberty of choice between digital and paper-based communication. According to the Bill, the duty will only be imposed on public authorities, thus giving the citizen the right to choose whether communication should be digital or on paper.

If the citizen wants to communicate digitally with public authorities, this will most frequently take the form of an application by e-mail, and the address for replying will appear automatically from the application. If the application is made non-electronically, an electronic address for replying may be included in the application.

However, private citizens and companies may have an interest in being able to indicate whether they wish to communicate digitally by registering at one central point, especially in connection with mass distribution or communication not caused by a previous application on the part of the citizen. So there will be a need of giving authorities access to the e-mail address of citizens who have thus expressed a wish to be able to communicate in a digital form. This presupposes that a central registration scheme should be arranged for e-mail addresses, which might be established conveniently in connection with the CPR and CVR registers.

It should thus be possible for citizens to indicate to public authorities or to other private citizens that they wish to place their e-mail address on an equal footing with their ordinary postal address in relation to public authorities, thereby undertaking the same duty with regard to their e-mailbox as their physical mailbox, namely the duty to empty the box and read incoming mail at regular intervals.

Subsections (2) and (3) will not be able to take effect until the registers in question have been arranged for it. It is therefore proposed to let these provisions become

effective subject to further decision by the Minister of Research and Information Technology.

Sections 18-23:

These provisions describe the extent of public supervision and the possibility of filing complaints regarding the decisions of the supervisory authority.

The National Telecom Agency will maintain general supervision of the operation and activities of authorized certification authorities so as to preserve confidence in the system. In case the certification authority fails to observe regulations for quality assurance and quality control, or the company fails to comply with the requirements stipulated under the Bill for carrying on such activities, the National Telecom Agency may revoke the authorization.

Supervision is expected to be carried out partly as concrete inspection of authorized certification authorities and partly by setting up and implementing system auditing. By system auditing is meant auditing of general computer control routines in certification authorities. System auditing implies that an external auditor approves the certification authority's procedures for computer control and makes sure that these are observed. Finally, the external auditor carries out regular evaluations of the computer control routines of the certification authority.

Furthermore the National Telecom Agency maintains supervision to ensure that non-authorized certification authorities observe the provisions of section 3(2), section 10 and section 12.

As described under the financial and administrative consequences of the Bill, it is the intention that public activities in connection with supervision should be financed by the user, a charge being collected from the authorized certification authorities to cover all expenses incurred by public authorities in connection with supervision, public registers in connection therewith and the development of competencies to be undertaken by the public sector in order to carry out adequate supervision, see section 16.

Section 21

To solve any conflicts between the user and authorized certification authorities, it is proposed to set up an administrative Appeals Board so that the individual user may receive justice without taking the matter into court, thus avoiding the consequent costs. However, as is the case with a number of other administrative boards, the Board cannot decide matters regarding compensation. The complaints facility is merely planned to involve a limited conduct-regulating fee, see section 22(4), no. 1, as is

known from other administrative complaints boards, e.g. the Consumer Complaints Board. The fee is not intended to cover the full costs of dealing with cases. Besides this fee, costs associated with the Appeals Board are covered by the fee collected from authorized certification authorities under section 19.

It is proposed that the Board should be composed of a person who meets the ordinary conditions for being a High Court judge, as the chairman, and four members who possess the necessary expertise within consumer questions, technology and finance. The Minister of Research and Information Technology will appoint the members subject to proposals submitted by relevant organizations. It should be noted that the Board is not intended to be composed with equal representation since this is a new type of enterprise where representatives of the industry as such cannot be appointed at the present time.

The decisions of the Board may be brought before the courts within six weeks. After this, the decisions of the Board will be final.

Section 24:

To ensure general confidence in digital communication via certification authorities, it is proposed that there should be a general possibility of imposing sanctions in case incorrect information is given to a certification authority regarding identities or similar matters. Sanctions under this Act will only be applied where more severe punishment is not prescribed under other laws. For example, false identity data given for the purpose of being able to carry out specific legal transactions with a third party in good faith may constitute fraud under the Civil Penal Code.

Section 25:

It is proposed that the Act should come into force on 1 January 1999. From the same date, it will be possible to grant authorizations to certification authorities.

Subsection (2):

Under section 17, public authorities and institutions have a duty to offer private citizens and companies digital messages. It is proposed that this duty should become effective at a date to be decided by the Minister of Research and Information Technology, but not earlier than 1 January 2001. During the period until the duty becomes effective, it is for the individual authority to decide whether it wants to offer citizens and companies this service.

Subsections (3) and (4):

At the moment is not possible to register an e-mail address either in the CPR or in the CVR register. The latter has not yet been established. It is therefore proposed that the Minister of Research and Information Technology should lay down more detailed conditions regarding the implementation of these provisions.