Bill on Electronic Signatures - Bill No. L 229

29. maj 2000

Bill No. L 229 introduced on 22 March 2000

Translation

Note: The text has been amended in section 5(2) and is therefore identical to the final text of Act No. 417 of 31 May 2000.

Only the Danish version of the text has legal validity.

Bill No. L 229

Danish Parliament (the Folketing)

1999-2000

Introduced on 22 March 2000 by the Minister of Research and Information Technology

(Birte Weiss)

Bill

on

Electronic Signatures 1)

Part 1. Scope and application ➦

1. The purpose of the Act is to promote secure and efficient utilisation of electronic communication by specifying requirements for certain electronic signatures and certification authorities that issue certificates for electronic signatures.

2.-(1) The Act shall apply to certification authorities established in Denmark that issue qualified certificates to the public, except as provided in section 12.

(2) The Act shall also apply to verification that signature-creation devices comply with the specified requirements for secure signature-creation devices.

Part 2. Definitions ➦

3. For the purposes of this Act:

1) "Electronic signature" shall be understood to mean data in electronic form that are attached to other electronic data by means of a signature-creation device and that are used to check that such data originate from the person indicated as signatory and that the data have not been changed.

2) "Advanced electronic signature" shall be understood to mean an electronic signature that:

(a) is uniquely linked to the signatory

(b) makes it possible to identify the signatory

(c) is created by means controlled only by the signatory, and that

(d) is linked to the data to which it relates in such a manner that any subsequent change made in the data is detectable.

3) "Signatory" shall be understood to mean a natural person who holds a signature-creation device and acts either on his own behalf or on behalf of another natural or legal person.

4) "Signature-creation data" shall be understood to mean unique data, such as a code or a private encryption key, which are used to create an electronic signature.

5) "Signature-creation device" shall be understood to mean a software- or hardware-based system used to implement and store signature-creation data.

6) "Signature-verification data" shall be understood to mean unique data, such as a code or public encryption key, which are used for the purpose of verifying an electronic signature.

7) "Signature-verification device" shall be understood to mean a software- or hardware-based system used to implement the signature-verification data.

8) "Certificate" shall be understood to mean an electronic attestation which links certain signature-verification data to the signatory and confirms the identity of same.

9) "Certification authority" shall be understood to mean a natural or legal person who issues certificates.

Part 3. Qualified certificates ➦

4.-(1) The designation "qualified certificates", or designations suitable for producing the impression that qualified certificates are implied shall only be used about certificates that meet the requirements stipulated in (2) and (3), and that are issued by a certification authority that meets the provisions of part 4 and rules laid down in pursuance thereof.

(2) A qualified certificate shall contain the following:

1) an indication that the certificate is issued as a qualified certificate

2) the name and domicile of the certification authority

3) the name of the signatory or a pseudonym, which shall be identified as such

4) any other information about the signatory that is needed for use of the certificate, including information that ensures unique identification of the signatory

5) the validity period of the certificate

6) a clear statement of limitations on the scope of use of the certificate, if applicable (scope limitations)

7) a clear statement of limitations on the transaction amounts for which the certificate can be used, if applicable (amount limitations)

8) the identity code of the certificate

9) the signature-verification data corresponding to the signature-creation data that were under the control of the signatory at the time of issuance.

(3) A qualified certificate shall be signed with the advanced electronic signature of the certification authority.

Part 4. Requirements concerning the activities of certification authorities ➦

5.-(1) A certification authority shall take the measures that are necessary for a secure, reliable and well-functioning offering of qualified certificates. The certification authority shall among other things:

1) apply administrative and management procedures that meet recognised standards

2) employ personnel who possess the required expert knowledge, experience and qualifications, including personnel with expertise in electronic signature technology and familiarity with proper security procedures

3) use trustworthy systems and products that are protected against unauthorised modification and ensure the technical and cryptographic security of the processes supported by them

4) take measures against any possible forgery of certificates

5) maintain sufficient financial resources at all times to operate in conformity with the provisions of this Act and to fulfil its liability obligations under the Act.

(2) Certification authorities that issue qualified certificates shall appoint an external state-authorised public accountant to undertake the system audit. In special circumstances the National Telecom Agency may exempt from the requirement that the system auditor must be a state-authorised public accountant.

(3) The Minister of Research and Information Technology shall lay down more detailed rules on the requirements in (1).

6.-(1) Certification authorities shall specify and apply adequate procedures for verifying the identity and any other facts concerning the signatory prior to the issuance of certificates.

(2) Information about the procedures mentioned in (1) shall be publicly available.

(3) The Minister of Research and Information Technology may lay down more detailed rules on the requirements in (1) and (2).

7.-(1) When issuing a qualified certificate, a certification authority shall ensure at the time of issuance that the signatory holds the signature-creation data corresponding to the signature-verification data given in the certificate.

(2) If, in connection with the issuance of qualified certificates, it is the certification authority that supplies the signature-creation and signature-verification data, only uniquely connected signature-creation and signature-verification data shall be used. The certification authority shall ensure confidentiality of the signature-creation data during the process of generation.

(3) A certification authority shall establish procedures for the issuance of certificates that make it possible to determine the date and time of issuance.

8.-(1) When entering into an agreement on the issuance of a qualified certificate, a certification authority shall inform the signatory in writing about the following:

1) The terms and conditions concerning the use of the certificate, including any limitations on the scope or amounts.

2) Any requirements concerning storage and protection of the signature-creation data by the signatory.

3) The signatory's cost of obtaining and using the certificate and of using the other services of the certification authority.

4) Whether the certification authority is accredited under a voluntary accreditation scheme.

5) Procedures for settlement of complaints and disputes.

(2) The terms of contract may be submitted electronically provided they are directly legible to the recipient.

(3) Relevant parts of the information given in (1) shall also be made available on request to third parties relying on a qualified certificate.

(4) The Minister of Research and Information Technology may lay down more detailed rules on the requirements in (1) to (3).

9.-(1) Certification authorities shall ensure the operation of a prompt and secure directory and a secure and immediate revocation service that makes it possible to check whether a qualified certificate is revoked, the validity period of the certificate or whether the certificate contains any limitations on the scope or amounts.

(2) A certification authority shall revoke a certificate immediately upon receipt of such a request from the signatory or if otherwise warranted by the circumstances.

(3) Information required under (1) shall be immediately available.

(4) A qualified certificate may only be made publicly accessible with the consent of the signatory.

(5) The Minister of Research and Information Technology may lay down detailed rules on the requirements in (1) to (3).

10.-(1) A certification authority shall record all relevant information concerning the certificates for an appropriate period of time, which shall be at least six years.

(2) A certification authority shall use trustworthy systems to store certificates in a verifiable form.

(3) Certification authorities must not store or copy signature-creation data of the persons concerning whom the certification authority have gained knowledge through the issuance of certificates.

(4) The Minister of Research and Information Technology may lay down more detailed rules on the requirements in (1) and (2).

Part 5. Liability ➦

11.-(1) Certification authorities issuing qualified certificates to the public, or guaranteeing

such certificates issued by another certification authority to the public, shall be liable to pay compensation for losses incurred by the person who reasonably relies on that certificate, if the losses were due to the following:

1) that the information contained in the qualified certificate was not correct at the time of issuance

2) that the certificate did not contain all information required under section 4

3) failure to revoke the certificate, see section 9(2)

4) lack of or erroneous information on whether the certificate has been revoked, the expiry date, or whether the certificate includes limitations on the scope or amounts, see section 9, subsections (1) and (3)

5) failure to comply with section 7.

(2) A certification authority shall be liable for damage in accordance with (1) unless the authority proves that it has not acted negligently or wilfully.

(3) A certification authority shall not be liable for:

1) losses occurring as a result of use of a qualified certificate outside the scope limitations applying to the certificate, or for

2) losses occurring as a result of violation of the amounts limitations applying to the certificate, provided that the limitations in question appear clearly from the certificate, see section 4, and that information concerning them is given on request, see section 9, subsections (1) and (3).

(4) Subsections (1) to (3) may not be departed from by prior agreement to the detriment of the injured person.

(5) Subsections (1) to (3) shall not apply if the loss is covered by the Act on Certain Payment Instruments.

Part 6. Supplementary requirements concerning the processing of personal data ➦

12.-(1) A certification authority may only collect personal data in connection with its activities directly from the person in question, or with the explicit consent of that person, and only insofar as the data are needed for the purposes of issuing and maintaining a certificate.

(2) Personal data collected under (1) must not be processed or passed on for any other purposes than those mentioned in (1) without the explicit consent of the person in question.

Part 7. Electronic signature and formal requirements ➦

13. Legal provisions according to which electronic messages shall be provided with a signature shall be regarded as met if the message is provided with an advanced electronic signature based on a qualified certificate and created by a secure signature-creation device. However, in the case of electronic messages to or from public authorities, this shall only apply if current legislation or provisions in pursuance thereof do not prescribe otherwise.

Part 8. Secure signature-creation devices ➦

14.-(1) A secure signature-creation device shall be understood to mean a signature-creation device that ensures by appropriate technical and procedural means that the signature-creation data used for signature generation:

1) can, in practice, appear only once

2) are reasonably certain to remain secret and cannot be derived

3) are protected against forgery, and

4) can be reliably protected by the signatory against unlawful use by others.

(2) A secure signature-creation device must not be designed in such a way that it changes the data to which an electronic signature is attached or prevents such data from being shown to the signatory prior to the signing.

(3) The requirements stipulated in (1) and (2) shall be regarded as satisfied if a signature-creation device meets generally recognised standards for such devices, which the Commission has laid down and published in the Official Journal in accordance with the procedure prescribed in Article 9 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

15.-(1) The Minister of Research and Information Technology shall designate one or more appropriate bodies or authorities that can assist in verifying that signature-creation devices comply with the requirements stipulated for secure signature-creation devices, see section 14, subsections (1) and (2), and will lay down detailed rules on the procedures for such verification and on the payment of fees for the same.

(2) A signature-creation device described as a secure signature-creation device may not be marketed or used to create advanced electronic signatures that are based on a qualified certificate until it has been verified, see (1).

(3) A verification of a secure signature-creation device by a body or an authority in another country within the European Economic Area (EEA) shall have the same status as a verification in pursuance of (1).

Part 9. Supervision ➦

16.-(1) Certification authorities shall notify the National Telecom Agency before or as soon as they begin issuing qualified certificates.

(2) The notification shall contain the following information:

1) name and domicile of the certification authority

2) corporate form if the certification authority is operated as a company

3) management and system auditor of the certification authority.

(3) Changes in matters reported in pursuance of (2) shall be reported not later than eight days after the change has taken place.

(4) The National Telecom Agency may lay down detailed rules on any other information to be included in the notification.

17.-(1) Together with the notification under section 16, the certification authority shall submit a report to the National Telecom Agency.

(2) The report shall contain the following:

1) a description of the certification authority's activities and systems

2) a declaration from the certification authority's management stating that its overall data, system and operation security must be regarded adequate and in compliance with the rules laid down in this Act and rules laid down in pursuance thereof, and

3) a declaration from the system auditor, see section 5(2), stating that, in the opinion of the system auditor, the certification authority's overall data, system and operation security must be regarded adequate and in compliance with the rules laid down in this Act and rules laid down in pursuance thereof.

(3) The certification authority shall prepare an updated report each year. The National Telecom Agency will set a deadline for submission of the report to the National Telecom Agency.

(4) The National Telecom Agency may lay down detailed rules on the content of the certification authority's reports and on how to perform system auditing in certification authorities.

§ 18. The National Telcom Agency shall ensure that this Act and rules issued in pursuance thereof are complied with.

(2) The National Telecom Agency may order a certification authority:

1) to notify the National Telecom Agency, see section 16

2) to report to the National Telecom Agency, see section 17

3) to bring matters concerning the certification authority's activities into conformity with the Act or rules issued in pursuance thereof.

(3) The National Telecom Agency shall stipulate a time limit for compliance with orders issued under (2).

(4) The National Telecom Agency may impose daily penalties on a certification authority for the purpose of enforcing compliance with orders issued in pursuance of (2), section 19(1) or section 20.

(5) The National Telecom Agency may require that an extraordinary system audit of a certification authority be carried out. The National Telecom Agency will appoint a system auditor to carry out the extraordinary system audit. The certification authority may be ordered to pay for the performance of the extraordinary system audit.

(6) The National Telecom Agency may deprive a certification authority of its right to use the designation qualified certificates, see section 4, if:

1) despite the imposition of daily penalties, the certification authority fails to comply with the National Telecom Agency's order in pursuance of (2), section 19(1) or section 20.

2) the certification authority has grossly or repeatedly violated the provisions of this Act or rules laid down in pursuance thereof, or

3) if the certification authority suspends its payments or goes into liquidation.

(7) A certification authority may request that a decision of the National Telecom Agency under (6) be brought before the courts. A request to this effect shall be received by the National Telecom Agency not later than four weeks after the date on which the decision was communicated to the certification authority. The National Telecom Agency shall bring a case against the certification authority under the rules of the Administration of Justice Act.

(8) A request to bring an action shall not have suspensive effect, but the court may decide that the certification authority in question shall have access to issue qualified certificates while the case is being heard. In the event of an appeal against a decision whereby the deprivation of the right to issue qualified certificates is found to be illegal, the court that made the decision, or the court before which the case was brought, may decide that the certification authority must not issue qualified certificates while the appeal case is being heard.

19.-(1) The National Telecom Agency may require the certification authority to submit all information found necessary for the Agency's supervision under section 18, including information to decide whether a natural or legal person is covered by such supervision.

(2) The certification authority and the system auditor shall immediately inform the National Telecom Agency of matters of vital importance to the certification authority's continued operation.

20.-(1) The National Telecom Agency may order a certification authority to choose another system auditor within a stipulated time limit, see section 5(2), if the present system auditor is found clearly unsuitable for his task.

(2) The National Telecom Agency may order a system auditor to provide information on matters concerning the certification authority without the consent of the certification authority.

(3) In the event of change of auditors, the certification authority and the withdrawing system auditor(s) shall each submit a report to the National Telecom Agency. The National Telecom Agency may order that the first sentence hereof be complied with.

21. The decisions of the National Telecom Agency under this Act or provisions laid down in pursuance thereof cannot be referred to other administrative authorities.

22. The Minister of Research and Information Technology may lay down rules to the effect that costs incurred in connection with the National Telecom agency's regulation shall be paid by the certification authorities that issue qualified certificates.

Part 10. International issues ➦

23. Qualified certificates issued by a certification authority established in a country outside the European Economic Area (EEA) shall be recognised in the same way as qualified certificates issued by certification authorities established in a country within EEA provided that:

1) the certification authority meets the requirements of this Act and is accredited under a voluntary accreditation scheme, or

2) a certification authority established in a Member State that meets the requirements of this Act, guarantees certificates issued by the certification authority in question, or

3) the certificate or the certification authority is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

Part 11. Criminal liability ➦

24.-(1) Unless more severe punishment is prescribed under other laws, penalty of fining shall be imposed on any person who:

1) violates sections 9(4), 10(3), 12 or 15(2)

2) gives wrong or misleading information to the National Telecom Agency, or

3) violates orders or decisions by the National Telecom Authority under section 18, subsections (2) and (6) and section 19 (1).

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

(3) The limitation period of criminal liability under (1) and (2) shall be five years.

Part 12. Coming into force etc. ➦

25. This Act shall enter into force on 1 October 2000.

26. This Act shall not apply to Greenland and the Faroe Islands but may by Royal Order be 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.

Footnote 1) The Act contains provisions that implement Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13 2000, p.12).

Explanatory Notes to the Bill ➦

General notes ➦

The purpose of the Act is to ensure that there will be electronic-signature products and certification authorities on the Danish market that will comply with a number of requirements that will make them secure to use.

From a socioeconomic point of view it is important to develop and provide electronic signatures of such a high security level that they are recognised in a broad forum and can be used to supply the provision of new services in both the private and the public sector.

The purpose of the legislation is not to control the overall provision of certification services. After implementation of the Act, the certification authorities will still be free to provide certificates and electronic-signature products without being subject to extensive regulation, authorisation schemes or being forced to apply specific technical solutions.

Thus the Act is intended solely to ensure the availability on the market of products (namely the qualified certificates described) for which a common minimum standard has been specified. In connection with the provision of electronic services where there is a need for authentication of the sender or recipient, both the private and the public sectors will thus have the possibility of requiring use of a certificate and an electronic signature that comply with certain minimum requirements.

At the same time, the legislation must ensure that the liability is clear when as a sender you use and as a recipient you trust a qualified certificate. The chosen liability model implies that it is the responsibility of the certification authority to prove that it has not made any mistakes in connection with the issuance of a certificate, revocation or when giving information about the expiry date and limitations on the use of the certificate.

A. Background and scope of the Bill ➦

1. The function and importance of electronic signatures ➦

The function and importance of electronic signatures can best be described by an example:

Agreements are often concluded by the parties signing a contract or by one of the parties, as confirmation of the conclusion of an agreement, delivering a note and invoice etc. to the other party.

In some cases the parties know each other in advance so neither of them will be in doubt about the identity of the other party. However, many agreements are concluded by parties that do not know each other in advance, and that will never actually meet as their communication takes place only by letter, fax or similar means.

When the parties communicate on paper, it is their signatures and perhaps a special letterhead that serve to identify the sender to the recipient. The paper also serves to ensure

that there will be no doubt later about the contents of the document used at the time of conclusion of the agreement. With paper-based communication the parties are thus able to see if an envelope has been opened while on the way and whether visible changes have been made to the written or printed text.

In practice, communication is usually exchanged without the parties giving much thought to these aspects and, in fact, it is only in a few exceptional cases that we need to pay attention to it.

When communicating through open digital networks, i.e. through networks that are accessible to everyone, such as the Internet, it is likewise essential to be sure with whom you are actually communicating and that the contents of the communication have not subsequently been changed.

When communication is electronic, there is no concrete evidence in the same manner that makes a recipient notice that the contents of a message may have been altered, and it is difficult, if not 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 an electronic message or to pretend to be somebody else without this being visible to the recipient.

An electronic signature is a combined "signature" and "lock" that may safeguard against these problems. In other words, an electronic signature locks a document with a content for a specific person after the signature has been attached.

The signatory can store the signature-creation data that are used to create the electronic signature on a plastic card or as part of a program on his PC. A password, which the signatory has, or some other kind of identification mechanism will usually be required to use the data.

The electronic signature is intended to safeguard both the signatory and the recipient, who does not know the sender in advance. In other words, the recipient of an electronic signature needs to be able to trust that the sender is in fact the person he claims to be and that the sender is still in possession of his signature-creating data (plastic card, computer program, etc.).

To ensure credibility vis-à-vis the recipient, the identity of the signatory must be verified by an independent third party, a so-called certification authority. In practice, what happens is that the certification authority after having verified the identity of the signatory issues an electronic certificate to that effect.

The certification authority must also establish a service function that allows the recipient to check automatically if a certificate, and thus an electronic signature, is revoked, for example if the signatory has lost possession of his signature-creation data.

The main purpose of the Bill is to lay down minimum requirements for certification authorities wishing to use the designation qualified certificates about the certificates they offer. Such certification authorities will be the only authorities entitled to use the designation and will be subject to, among other things, increased liability for the data in a certificate being correct and adequate and for the correct functioning of the certification authority's revocation function.

It is not a question of authorisation or approval of certification authorities, but such authorities will be subject to regulation by a public regulator, who may require regular

documentation for compliance with the Act, and who may apply various sanctions if a certification authority does not comply with the requirements of the Act.

2. What is an electronic signature, an electronic signature certificate and a certification authority? ➦

In practice, an electronic signature is based on two elements.

The first element is the so-called key pair, which can be described as two halves of a key, a code or a lock. The signatory has one half (the private key) and an independent certification authority stores or registers the other half (the public key).

The second element is a certificate issued by an independent certification authority; the certificate verifies the identity of the signatory and states that the signatory has possession of the private key that matches the public key contained in the certificate and which may be used by the third party to verify and prove that he has in fact been communicating with the signatory.

With the technology of today, communication will then take place as follows: the signatory sends an electronic message, which may consist of a text file, graphics, a sound recording, a spreadsheet or the like, or a combination of several of these elements. When the signatory is ready to send his message he attaches his electronic signature by means of his signature-creation device (plastic card, computer program, etc.) and his private key. The affixation also "locks" the document so that when the message is opened later, it will be possible to see whether subsequent attempts have been made - by the sender, recipient or third party - to change it.

Then the signatory sends his message to the recipient. He will also often attach his certificate containing the attestation of the certification authority together with his public key, which the recipient needs in order to check the message.

However, it may be that the sender has lost possession of his certificate and his private key or that the certificate has expired and can therefore no longer be used. To check this, the recipient will have to contact the certification authority and request them to confirm that a user's certificate has not been revoked in the same way as a payment card. The certification authority will also be able to tell the recipient if the certificate has expired and if there are any limitations on what the signature can be used for or limits on the value of transactions for which the signature can be used.

In a number of cases, both the sender and the recipient may need to prove when they sent, received or verified a message assigned an electronic signature. In this regard, the certification authorities may, as independent third parties, offer a facility whereby electronic messages are forwarded for time stamping, possibly as part of the process of sending the message to the recipient (a kind of "mail stamping function") or immediately after receipt of the message. The extent to which such facilities will be offered in practice will depend on the demand.

The certification authorities will usually be commercial enterprises, although public authorities, organisations etc. may also decide to set up a certification function. The type of products offered by the individual certification authorities will differ. Some certification authorities will only offer issuance of certificates and thus expect the customer to obtain the actual electronic signature (the key pair) elsewhere. Others will offer both. Other certification authorities, although probably not all of them, will offer time-stamping functions.

There may also be wide differences as to how the certification authorities are set up in practice, including their use of IT solutions and security procedures.

An enterprise serving as a certification authority may also carry out activities in a number of other areas. An obvious example is activities within credit and payment cards or other forms of financial activities or mail handling.

It should also be emphasised that what we have is a market and some products that are only just being developed and that the technology used is constantly changing. This also means that the above description of how an electronic signature and electronic signature certificates operate today is no more than an outline that might not necessarily be true in one, five, or ten years' time.

3. User interest in the use of electronic signatures and electronic signature certificates ➦

As mentioned earlier, the users' main interest is that when communicating through open digital networks, such as the Internet, he wants to be sure who he is actually communicating with and that the contents of the communication have not been changed in transit or later. Another decisive element is to be able to prove subsequently what has happened and when.

From a user's point of view, security - both as sender and recipient - depends on the following:

(i) How and how thoroughly does the certification authority verify the identity of the signatory prior to the issuance?

(ii) How secure and thorough are the certification authority's procedures as regards registration of and information on the revocation or expiry of certificates and digital signatures, or on certificates containing limitations on use?

(iii) Is the above information of a certificate correct and adequate?

(iv) What is the liability of certification authorities in situations where a certificate is incorrect on one or more of the above-mentioned points, or where errors have occurred in other ways at a certification authority, resulting in losses for either the sender or the recipient?

(v) How is the quality of the electronic signature used in connection with a certificate, i.e. is it in fact possible to break or copy the signature without leaving any visible traces?

The importance of the above-mentioned issues depends on the desired use of the signature.

4. In which contexts will electronic signatures and electronic signature certificates be used? ➦

The rapid development in recent years within information technology, including the merging of electronic data processing and telecommunications, has led to increased use of digital communication in all spheres of society. The use of electronic mail, information exchange and a number of other forms of transactions via the Internet is rising sharply.

In relation to public authorities, electronic communication enables more efficient

communication between authorities and private citizens and enterprises. For example, more and more digital self-service systems are being developed that allow citizens to file their tax returns, apply for study grants, 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., from a PC at home or at work, or from a public information kiosk.

The Ministry of Research and Information Technology's pilot projects on the use of electronic signatures in public services include a number of practical examples on how electronic signatures can be used in combination with, for example, student cards, payment and reports on student grants, exchange of information on patients, patient records and the settling of health insurance accounts between a number of health institutions. The experience gained from the pilot projects is of great importance to the design of a universal infrastructure for electronic signatures. The projects have revealed many of the problems that arise when electronic signatures are used in practice.

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).

Today, electronic data interchange between companies is carried out in a number of situations in dedicated systems where security aspects, exchange formats etc., have been agreed in advance between the parties involved. The common standards for electronic data interchange serve as an example of a code of practice that may be used in such dedicated systems. Companies doing business with each other on a regular basis have found it useful to set up such framework agreements. However, this solution is not feasible if the aim is, in principle, for all companies, authorities and private individuals on the network to be able to carry out legally binding transactions with each other - for example placing an individual order or entering 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 provides a satisfactory framework for carrying out legally binding transactions via open networks such as the Internet without having to arrange with the recipient in advance how to do it.

However, the Danish business community is not the only sector that is interested in electronic communication. Private citizens also increasingly want to use the Internet in a commercial context, i.e. for ordering and buying goods and services via the Internet.

Today, communication as mentioned above already takes place in some situations without any use of electronic signatures. This applies particularly to less complicated transactions. Also in situations in which someone wishes to use and electronic signature, there are differences in the economic risks and possible losses etc. that may occur.

As a result, there is a trend towards the development of electronic signatures and associated certificates with graduated security tailored for different types of use.

Thus it is likely that an individual citizen will have different digital certificates and signature-creation devices at his disposal for different purposes, for instance for small private purchases, for communication with public services, or in a work context.

It should largely be left to the market itself to arrange for certification authorities to be

established and to ensure that the solutions they offer are sufficiently secure for the situations for which they are intended. The reason is that this is still a rapidly developing market - and one in which too much government regulation is certain to impede product development. In addition, any such regulation would have to be constantly updated in step with the latest technical advances.

However, this is a new market with products of such technical complexity that it is extremely difficult for the individual private user to be sure that the product offered has the necessary security.

At present, there is no regulation of enterprises that wish to offer certificates and electronic signatures.

5. The significance of legislative regulation on electronic signature certificates ➦

The main purpose of the Bill is to establish a flexible regulation and control scheme for certification authorities that wish to offer certificates with the designation qualified certificates and, in that connection, to regulate the liability of the certification authorities in question to signatories and recipients of qualified certificates.

The regulatory scheme means that the certification authorities covered by it must currently document that their activities and the certificates they issue comply with a number of minimum requirements to ensure a range of solutions of the necessary quality on the Danish market. The minimum requirements to be set up comprise points (i)-(iii) in paragraph 3 above, i.e. to ensure the quality of electronic signature certificates. If the rules are not complied with, a certification authority may be deprived of its right to use the publicly recognised designation qualified certificates for their certificate products.

As far as concerns regulation of the extent of a certification authority's liability for errors due to non-compliance with the stipulated minimum requirements (point (iv) in paragraph 3), the aim is fault liability with reversed burden of proof.

The regulatory scheme and regulation of liability will not cover all certificates offered or all certification authorities in the market, but only certificates that a certification authority chooses to call "qualified certificates". As part of its overall activities, a certification authority will be able to offer qualified as well as other certificates, including certificates that comply in principle with the minimum requirements of the Act but that are not called qualified certificates.

The Bill covers certificates used for publicly accessible systems, but not solutions used only for dedicated networks where a specific code of practice has been agreed between the parties involved. So this kind of use of electronic signature certificates is not covered by the rules on regulation and liability.

6. The role of legislative regulation on electronic signatures ➦

The regulatory scheme described above and the associated regulation of liability concern the actual issuance of electronic signature certificates by the certification authorities.

As described above in paragraph 2, there is another important security aspect of the use of electronic signatures, i.e. the quality of the actual key pair used (also called the signature-creation and signature-verification data), and the way in which the private key in particular is used and stored (on a plastic card or as part of a PC program) (also called the signature-creation device).

In some cases, but not all, the certification authority will also have supplied the signature-creation product.

In accordance with the underlying EC Directive on a Community framework for electronic signatures (the Directive has been included as Annex 1 to the Bill, hereinafter referred to as the "Directive" or the "EC Directive"), the Bill lays down a number of basic requirement concerning signature-creation devices that the manufacturer/supplier wishes to call "secure signature-creation-devices" as defined in the EC Directive. In extension of this, the Bill provides authority for the designation of one or more appropriate bodies or authorities that can help to verify and document that specific products comply with these minimum requirements.

The minimum requirements in question are formulated in very general terms and are primarily functional minimum requirements aimed at ensuring, to the widest possible extent, a technology-neutral and thus robust regulation. This is necessary because the technology used - or several competing technologies - are still at a relatively early development stage, where technological solutions are constantly changing, and thus make it impossible to implement stable regulation and to lay down highly specific technical minimum requirements.

It is also possible, as part of the development in question, that authentication methods will in time be developed that might replace all the digital signature solutions that we know today.

The "labelling" of specific signature-creation devices thus enabled will guide users who wish to procure a product they can rely on and is also important to the regulation of the problems of legal effect, see paragraph E, point 9 below.

B. Existing legislation ➦

At present, there is no legislation on the issuance of certificates that can be applied to electronic signatures (certification authority activities) in Denmark. Certification authorities lay down their own rules for the issuance of certificates and for how to verify the identity of signatories, and are not subject to any particular compensation scheme if certificates are faulty, are not revoked in time, etc.

If mistakes are made in connection with the issuance or use of a certificate that links the signatory and the electronic signature, the matter will at present have to be tried in accordance with the general law of damages. This means that injured parties will have to prove that a certification authority has made mistakes in connection with its issue or handling of a certificate.

C. Danish initiatives on electronic signatures ➦

On 28 January 1998, the Minister of Research and Information Technology, as the minister primarily responsible, together with the Minister of Trade and Industry, the Minister of Economic Affairs and the Minister of Taxation, presented a report to the Folketing (the Danish parliament) on the security of digital communication.

The point of departure of the reports was a noted substantial demand from the commercial sector, public authorities as well as private users for legal regulation that will provide a satisfactory framework for making legally binding transactions via the Internet.

The parliamentary debate showed an express wish to create a legal framework for the use of electronic signatures that will ensure high quality and thus establish the basis for practical equality between digital and paper-based communication. It was emphasised that use of electronic communication for binding legal transactions depends on certainty concerning the identity of the sender and the recipient, the integrity of the content and, often, guaranteed confidentiality in relation to other parties as well. In other words, solid technical solutions must be available.

The debate also showed that there is a need through legislation to be able to deal with the liability of certification authorities. It was the general view that the issue should be dealt with from the point of view of the consumers. The regulation must result in secure, but also simple and user-friendly devices, and a balance must be struck between protection of the users and definition of the liability of certification authorities. It was considered desirable to provide the required legal basis for establishing certification authorities that can provide solid quality solutions and clear rules on certification authorities' liability and compensation in connection with the issuance of certificates for use in combination with digital signatures.

Based on the parliamentary debate in February 1998, the Ministry of Research and Information Technology circulated a draft Bill on digital signatures for public consultation. The Bill contained two main elements. The first was a proposal for an authorisation scheme with a number of minimum requirements for digital signature certificates and certification authorities wishing to obtain authorisation, and the seal of approval that would thus be implied. The authorisation scheme was to be combined with restrictive regulation of the liability of certification authorities in situations where the publicly regulated minimum requirements were not complied with, in the form of absolute liability for loss occurring as a result.

The second was a proposal for regulation of the legal effects of using digital signatures by way of equal status for digital and written signatures. The Bill contained two alternative models on how the latter might be implemented in practice.

The result of the consultation on the first Bill made it clear that it was necessary to consider further the issue of possible regulation of the legal effect of digital signatures in areas with statutory requirements for signatures or existence in writing, etc. The consultation also made it clear that considerations on such legislation would be closely bound up with a number of legal problems across the board and would, among other things, affect general property contract and tort law, general law of contract, and consumer protection law that come within the sphere of the Ministry of Justice.

Consequently, it was decided to divide the legislation work on the use of electronic signatures and electronic signature certificates between the Ministry of Justice and the Ministry of Research and Information Technology, with the former responsible for regulation of problems in connection with the legal effects of using digital signatures. For this purpose, the Ministry of Justice has set up a committee with representatives from the Ministry of Research and Information Technology, which is to consider more closely the need to legislate on the extent to which electronic messages can/must be used in areas with formal requirements as mentioned above and on the legal effects between sender and recipient in certain defined situations. The committee has not yet completed its work.

The result of the consultation also made it clear that there was a need for further work on the Bill's provisions on authorisation and liability and for the provisions to be seen in an international perspective, especially as the market for certificates and electronic signatures will be largely international and be characterised by transboundary solutions. Consequently some of the consultation replies also pointed to a need to harmonise Danish regulation with regulation in other countries if it was desired to promote the establishment of certification

authorities in Denmark as well.

D. International developments ➦

Establishment of a framework for electronic signatures is not an isolated Danish phenomenon. Such systems must also to a great extent be able to function globally if the business community and users are to benefit fully from the facilities offered by the systems.

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

Internationally, regulatory activities concerning electronic signatures have primarily been concentrated around the International Chamber of Commerce, OECD and UNCITRAL (United Nations Commission on International Trade Law), and the EU.

The EC Directive on a Community framework for electronic signatures

The Directive was adopted on 13 December 1999 and is a follow-up on two communications from the Commission on electronic commerce and on encryption and digital signatures from April and October 1997, respectively.

The main points of the Directive ➦

The background of the Directive is the Commission's view that a prerequisite for accelerating electronic commerce is the establishment of 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 recipient in advance how to do it. Use of electronic communication for binding legal transactions presupposes that it is possible to communicate with certainty of the sender's identity and certainty that the content has not been changed.

The purpose of the Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. The Directive provides a framework for electronic signatures and associated certification services etc. so as to make the internal market secure with respect to electronic signatures.

Scope ➦

The scope of the Directive is electronic signatures. The Directive operates with a broad definition of an electronic signature since it defines an electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

The Directive also operates with the concept "an advanced electronic signature", which is an electronic signature that must be 1) uniquely linked to the signatory, 2) capable of identifying the signatory, 3) created using means that the signatory can maintain under his sole control, and 4) linked to the data to which it relates in such a manner that any subsequent change made in the data is detectable.

The distinction between an electronic signature and an advanced electronic signature is significant to the Directive's provisions on legal effects (see below).

It is left to the Member States to decide in their national law the legal spheres in which electronic documents and electronic signatures may be used.

Electronic communication in dedicated systems is not covered by the general regulation of the Directive. In cases where the parties have concluded a communication agreement in advance, such an agreement is given precedence. However, electronic signatures given within such systems must not be excluded from obtaining the legal effects provided by the Directive.

Specification of a number of requirements concerning certification authorities and electronic signatures ➦

In order to create a market for high-quality electronic signatures and with the same level of security within the entire EU, the Directive lays down a number of requirements concerning service providers (in the Directive certification authorities are called certification service providers) of so-called qualified certificates for electronic signatures. In the following review of the Directive, the Directive's designation for these certificates will be used.

In the Directive "certification authorities" means a person or an entity who issues certificates or provides other services related to electronic signatures to the public. This means, among other things, that service providers that do not offer certification are still covered by some of the Directive's rules if they offer "associated" services such as time stamping of electronic mail. The Directive specifies in Annex II a number of basic requirements concerning such service providers.

According to the Directive, a certificate for an electronic signature is a digital attestation that links signature-verification data to a person and confirms the identity of that person.

According to the Directive, a qualified certificate means a certificate that meets the requirements laid down in Annex I and is provided by a certification authority that fulfils the requirements laid down in Annex II.

The Directive lays down rules for the certification authority's liability to "any person who reasonably relies on the certificate". The European Commission has stated that these persons also include the signatory.

The liability rules cover only cases in which a certification authority has issued a certificate as a qualified certificate or in which the service provider guarantees a certificate of another service provider.

The certification authority must be responsible for 1) the accuracy at the time of issuance of all information contained in the certificate, 2) assurance that at the time of the issuance of the certificate, the person identified in the qualified certificate held the signature-creation data (the private key) corresponding to the signature-verification data (the public key) given or identified in the certificate, and 3) assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases in which the certification authority generates them both.

The liability rules must be based on a principle that certification authorities must at least have acted negligently in the three cases mentioned above. According to the Directive, it is for the certification authority to prove that it has not acted negligently.

Member States must also ensure that certification authorities that issue qualified certificates are liable for damage caused as a result of failure to revoke certificates unless the

certification authority proves that it has not acted negligently.

The Directive contains no regulation of the liability between the signatory and the recipient of an electronic signature.

The Member States must ensure that certification authorities and national bodies responsible for accreditation or regulation comply with the general EC Directive 97/46/EC on personal data protection. It is provided that the certification service provider may only collect personal data directly from the person in question or with the explicit consent of that person. Personal data may only be collected insofar as the data are needed for the purposes of issuing and maintaining a certificate.

An open market ➦

The Directive prohibits prior authorisation of certification authorities as a condition for providing certification services for electronic signatures.

Prior authorisation should be understood to mean any licence, the issuance of which requires a decision by the national authorities before the certification service provider can offer its certification services, and any other measure with the same effect.

This is to ensure that the certification authorities are able to offer their products across the EU, thereby strengthening competition in this special area to the benefit of the consumers and the business community. It must be assumed that this will result in the consumers and the business community being offered a number of products that afford new possibilities of secure electronic exchange of information. A free market will thus stimulate Community-wide provision of certification services.

However, the Directive makes it obligatory for the Member States to establish an appropriate regulation of the certification authorities that issue qualified certificates for electronic signatures. The Directive opens the way for the Member States to leave the establishment of such systems to the market players in the form of self-regulation.

The Member States must recognise certificates issued by certification authorities of countries outside the European Economic Areas on an equal footing with certificates issued by certification authorities within the EEA provided 1) third-country certification authorities fulfil the requirements of the Directive and have been accredited under a voluntary accreditation scheme established in an EU country, 2) if an EU certification authority that fulfils the requirements of this Directive guarantees the certificates of the third-country provider, or 3) if the third-country certificate or third-country provider is recognised under an international agreement.

Legal recognition of electronic signatures ➦

The Directive contains some rules on the legal effects of electronic signatures. The Directive thus contains a ban on "discrimination" of electronic signatures with respect to legal enforceability and admissibility as evidence in legal proceedings solely on the grounds that the signature is electronic or fails to comply with certain security requirements.

This "discrimination ban" means that the Members States must not deny electronic signatures legal effect etc. solely on the grounds that they are in electronic form. The ban does not mean, however, that Member States cannot treat electronic signatures differently from hand-written signatures for other reasons. If, for example, an electronic signature has been generated by a technology that affords only limited protection against forgery etc. it

will not conflict with the "discrimination ban" to treat such signatures differently from hand-written signatures due to the low level of security.

The Directive also contains a provision to the effect that the above-mentioned "advanced" electronic signatures, i.e. electronic signatures that comply with particularly strict security requirements must be deemed to meet formal requirements for signatures on paper documents. However, this applies only if a Member State accepts the use of electronic signatures in that context.

As mentioned above, it will still be for the Member States to decide in which areas they will accept the use of electronic documents and electronic signatures. However, the provision means that, in areas where national law requires a signature on electronic messages, the Member States must accept that advanced electronic signatures fulfil this requirement. In the case of communication with public authorities, however, the Directive enables Member States to make more stringent security requirements for electronic signatures provided they are objective, transparent, reasonable and non-discriminatory.

Finally, the Directive contains a rule to the effect that Member States must ensure that "advanced" electronic signatures can be used as evidence in legal proceedings. The preamble of the Directives makes it clear that the rules do not change the principle regarding the unfettered judicial consideration of evidence.

The Danish procedure in respect of the Directive ➦

The Draft Directive was presented to the Parliamentary Committee on European Affairs on 15 May 1998 together with the Ministry of Research and Information Technology's Memorandum of 7 May 1998 prior to the Council meeting (on telecommunications) on 19 May 1998.

The Draft Directive was also discussed in a consolidated memorandum of the Ministry of Research and Information Technology of 13 November 1998 with a view to informing the Parliamentary Committee on European Affairs prior to the Council meeting (on telecommunications) on 27 November 1998. And the Draft Directive was referred to in a report to the Parliamentary Committee on European Affairs on the Council meeting (on telecommunications) on 27 November 1998.

Nordic cooperation on legislation on electronic signatures ➦

The Ministry of Research and Information Technology has participated in informal cooperation between the relevant authorities in Norway, Sweden, Finland and Iceland with a view to exchanging experience and endeavouring to create conformity where possible with the legislation in the individual countries.

Sweden has sent out a new draft Bill on certificates for electronic signatures for consultation and expects to be able to introduce a new Bill in the Swedish parliament (Riksdagen) in a few months' time.

The Swedish draft is in many ways identical to the present Bill. Unlike the present Bill, however, Sweden wants a less comprehensive regulatory scheme based on the principle that certification authorities wishing to issue qualified certificates themselves declare that they comply with the statutory requirements. The Swedish National Post and Telecom Agency (Post- og Telestyrelsen) has been suggested as supervisory authority. Certification authorities would be required to submit information with a view to enabling the supervisory authority to check compliance with the Act.

Norway has just sent out a draft Bill on electronic signatures etc. for public consultation and expects to introduce a Bill in the Norwegian parliament (Stortinget) in the autumn. The Norwegian draft, like the Swedish, resembles the present Bill in many ways. Norway has chosen a supervisory model that resembles the Swedish model because it does not wish to impose to heavy administrative burdens on the certification authorities.

Finland and Iceland are also presently engaged in completing a draft Bill to be sent out for public consultation. Finland has already implemented parts of the 1998 Directive by adopting an act on electronic communication.

Other international initiatives ➦

In 1997, the International Chamber of Commerce issued a set of guidelines on best practice within certification and safeguarding of electronic commerce. The primary target group of the guidelines is the business community and its business-to-business trade.

The guidelines are mainly based on UNCITRAL's model law on electronic commerce.

The UN Commission on International Trade Law (UNCITRAL) adopted a model law on electronic commerce in June 1996. 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 provided that the functions served by paper are served equally well digitally. 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 states that information must 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 states 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 recommendation of 27 March 1997, the OECD encouraged its Member States to remove or avoid creating unnecessary obstacles to digital communication for the sake of an encryption policy.

Also in 1997, the OECD published a report on certification in the electronic environment together with another report on technological capabilities of certification of data in a global network. This report was followed by yet another report in 1998. These documents provide an overview of the trend in technological developments and important political areas within this field.

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 other 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, Germany, France and Austria have adopted national legislation on electronic documents/contracts and digital signatures.

To summarise, the situation can be described as follows: there are a number of initiatives under way, both nationally and within the framework of international cooperative bodies. The EC Directive on electronic signatures serves as a clear landmark indicating in which direction international regulation is moving.

E. The contents of the Bill ➦

1. The scope of the Act ➦

The territorial scope of the Act is certification authorities established in Denmark. The Act does not specify any special requirements concerning certification authorities and electronic signatures originating in other countries within the EU, or in third countries outside the EU, but does make it possible for certificates issued by them to be recognised in the same way as certificates issued by Danish certification authorities.

The Act will not apply to certificates and electronic signatures used exclusively within dedicated systems based on voluntary agreements between a limited number of participants

2. Technology-neutral regulation ➦

The Bill is based on a wish to ensure technology-neutral and robust regulation.

In extension of this, the Bill's scope is electronic signatures and not only digital signatures, which constitute the present predominant technology.

An electronic signature is a technical means giving the same function as an ordinary handwritten signature, i.e. relating a certain amount of data to a specific person. Electronic signatures occur in several variations.

A digital signature is at present the main technical solution for an electronic signature. A digital signature guarantees the sender's identity and that the message has not been changed on the way (integrity). A digital signature is produced by means of a computer program based on the use of public-key encryption techniques.

Public-key encryption is a special form of encryption. Encryption is a technique for scrambling data according to a specific principle. For example, each letter of a text can be replaced by another letter further ahead in the alphabet. In the example mentioned, the same key is used both to scramble and restore the text. Public-key encryption, however, uses two different but linked keys so that a text that has been encrypted with one of the keys (no matter which), can only be decrypted by the other key. The name "public key" stems from the fact that with such a system one can establish a certification authority with which one of the keys (the public key) is registered, and which verifies the identity of the person in possession of the key in question, to potential communicating parties. Public-key

encryption thus ensures a high degree of certainty of the sender's identity without having to agree on the code or exchange keys in advance.

It is thus considered important that the Bill cover not only digital signatures but also future techniques that serve the same purpose as the public-key-encryption technique and thus also other forms of digital identification.

For this purpose, the Bill operates with a broad definition of an electronic signature since it defines an electronic signature as data in electronic form that are attached to or logically associated with other electronic data and that serve as a method of authentication (identification).

It is important to emphasise that the electronic signature market, like so much else in the IT world, is characterised by rapid technological development which makes it difficult to predict how it will actually develop. This also means that the picture of technological capabilities and functionalities is constantly changing, which makes extensive and technology-specific regulation impossible.

3. General certificates versus qualified certificates ➦

The Bill specifies a number of requirements for certification authorities offering so-called qualified certificates. The requirements cover both the contents of a qualified certificate and the procedures used by the certification authorities. The requirements are intended to ensure a high level of security in connection with the issuance and administration of these certificates.

A qualified certificate is a certificate that contains the information required in section 4 of the Bill and is issued by a certification authority that complies with the provisions of Part 4 of the Bill and the rules issued in pursuance thereof.

The provisions include an implementation of the requirements made in the Directive on the provision of "qualified certificates".

If a certificate includes an indication that the certificate is issued as a qualified certificate, and if the issuing certification authority is domiciled in Denmark, then the requirements in this Act on the provision of qualified certificates must be met.

A qualified certificate must include data that make it possible to identify the signatory. The signatory (i.e. the person generating the signature) is the natural or legal person stated in the certificate. It is the person that controls a signature-creation device and holds the signature-creation data (the private key).

4. Requirements for certification authorities offering qualified certificates for electronic signatures ➦

Part 4 of the Bill includes a number of requirements for certification authorities offering qualified certificates for electronic signatures.

The provisions require providers of qualified certificates to take the legal, organisational, technical, personnel, operating and security measures required to make them secure and well-functioning providers of electronic signatures.

To achieve this, the certification authorities issuing qualified certificates must employ

personnel that possess the required expert knowledge, experience and qualifications for the services provided. This may differ from one service provider to another depending on the services provided. The personnel must possess expertise within electronic signature technology and know how to establish and maintain adequate and proper security procedures. The personnel must be familiar with the systems and products used.

In addition, the certification authorities must maintain sufficient financial resources at all times to comply with the provisions of this Bill and to fulfil their financial liability in pursuance of the special liability regulation. Whether a certification authority has sufficient financial resources for this will depend, among other things, on the type of certificates offered. If, for example, a certification authority offers certificates for use within an area of high economic risk for the parties involved or offers certificates without limitations on the scope or amounts, then the financial resources must be equally large.

Finally, as an important key element of the regulation, a certification authority must comply with certain minimum requirements on how the identity of a signatory is to be verified prior to the issuance of a qualified certificate in order to secure adequate checking thereof. This identity check, together with the rules ensuring adequate procedures for the certification authorities' design, storage and administration of certificates, constitutes the core of the regulation of qualified certificates. This regulation is described in more detail in the notes on section 6 of the Bill.

The system auditor, who, according to the Bill, must be attached to the certification authority, must submit annually to the National Telecom Agency a report on whether, in his opinion, the certification authority observes the stipulated rules and requirements, and the management of the certification authority must guarantee that.

The Bill specifies the general rules on the requirements made concerning certification authorities that provide qualified certificates. The Bill authorises the Minister of Research and Information Technology to lay down specific rules on the precise content of the requirements made concerning certification authorities in a number of the above-mentioned areas.

5. Regulation and notification ➦

The National Telecom Agency is assumed to maintain general regulation to ensure that certification authorities comply with the rules of this Act.

The National Telecom Agency must check that the requirements of this Act, concerning both certification authorities and the certificates they issue, are complied with. The requirement that certification authorities issuing qualified certificates be subject to regulation by a public regulator is intended to ensure that these certification authorities maintain a quality and security level with which users can be confident.

The main task of the National Telecom Agency will be to assess the audit reports to be submitted by certification authorities when they start operating and in connection with their annual presentation of accounts.

If the information that the National Telecom Agency receives from a certification authority, its auditors, users or others causes doubt about whether the certification authority complies with the requirements of the Act, the National Telecom Agency has a number of recourses described in the Act.

Unlike today's regulation of companies in the financial sector, it is not intended that the

National Telecom Agency should actually inspect the companies subject to regulation.

The National Telecom Agency's recourses include the right:

I. to require a certification authority to submit all the relevant information needed for its regulation

II. to order a certification authority to bring specific matters in conformity with the legislation

III. to impose daily penalties if a certification authority fails to comply with an order

IV. to arrange for an extraordinary audit of a certification authority to be carried out, and

V. to deprive a certification authority of its right to use the designation "qualified certificates" about its products.

It is not considered necessary to give the National Telecom Agency the right to carry out inspections of the premises of certification authorities.

Certification authorities that do not wish to issue qualified certificates will be able to establish themselves freely and operate in accordance with quality requirements and standards decided upon by themselves. The National Telecom Agency will, however, also check that the Danish certification authorities observe the provisions of section 12 concerning processing of personal data.

By letting the market for electronic signatures be open to players that do not meet specific requirements concerning regulation etc., it is ensured that a potential market development in which private authorisation schemes or similar schemes will prevail is not impeded by inflexible legislation.

The reasons for organising the regulation as an audit-based system in which a major part of the practical regulation is carried out by the external auditor at the certification authorities, are first of all to make use of the experience and competence in the performance of system audits that already exist in the audit sector. Expert knowledge is required to be able to understand and assess the advanced technology used by a certification authority and the National Telecom Agency does not possess that knowledge today.

Secondly, it will take a great deal of resources to build up extensive governmental regulation, and it is assumed that these will be paid for by the companies subject to regulation. This might deter certification authorities from issuing qualified certificates, which would mean that the quality of the market created for electronic signatures might be insufficient to inspire confidence among consumers, authorities and companies. It is believed that the cost of the audits imposed by the Bill on the certification authorities will be of far greater benefit to the certification authorities themselves in the form of knowledge, control and exchange of experience with the auditors than would be the case with a governmental scheme.

It is proposed that the costs of the regulation be financed by the public sector in the short term, but in the longer term they should be paid by the certification authorities that issue qualified certificates.

6. Liability rules ➦

Section 11 of the Bill specifies special liability rules for certification authorities that issue qualified certificates.

The provisions specify the liability in specific cases where a person who reasonably relies on a certificate suffers a loss due to a certification authority. These are cases such as losses incurred as a result of errors and deficiencies in the certificate data, failure to revoke a certificate, lack of or erroneous information on the expiry date or applicable usage limitations on certificates, as well as errors in the certification authority's verification that a signatory holds the signature-creation data corresponding to the signature-verification data given in the certificate.

According to the provisions, it is for the certification authority to prove that errors have not occurred that can be attributed to the certification authority in connection with the issuance of a qualified certificate for an electronic signature and that the information in the certificate is correct.

It is also the responsibility of the certification authority to make information available on a certificate's expiry date, revocation, limitations on its use or limits on the value of transactions for which the certificate can be used and that such information is correct.

So in this case there is fault liability with reversed burden of proof, or presumption of negligence. The reason for introducing this increased liability for certain certification authorities is the highly technical and complicated nature of the area. It will be difficult for the ordinary user of electronic signatures to prove that errors have occurred in the handling of the signature services. The rules thus aim to protect consumers. In order to impose liability on a certification authority for a loss suffered by the signatory or a third party under the provisions of this Bill, the other conditions for imposing liability must exist.

Matters that are not covered by the special increased liability in this Act will be decided according to the ordinary rules of Danish law.

7. Protection of personal data ➦

The Bill contains a few supplementary provisions to the existing legislation on protection of personal data.

The provisions in the Bill on protection of personal data apply to all certification authorities established in Denmark.

According to the Bill, a certification authority may only collect personal data in connection with its activities directly from the person in question or with the explicit consent of that person, and only insofar as the data are needed for the purposes of issuing and maintaining a certificate.

A certification authority must not pass on or process data for any other purpose than required for issuing or maintaining a certificate without the explicit consent of the person in question. This ensures that data collected by a certification authority without the consent of its customers cannot be used for marketing purposes etc.

8. Secure signature-creation devices ➦

As described above in section A, subsection 5, the Bill also contains specific regulation of the minimum requirements for signature-creation devices, which certification authorities

want to call "secure signature-creation devices". The basis for this is Annex III of the EU Directive, which contains a number of functional minimum requirements for such signature-creation devices. The Directive also provides authority for the European Commission together with the Member States to decide which generally recognised international standards for such devices are deemed to meet the minimum requirements of the Directive. To the extent that such amplifying regulation is implemented, it will, according to the Bill, constitute the basis also for verification by Danish authorities etc. as to whether specific products meet the stipulated minimum requirements.

It is also intended that the European Commission, together with the Member States, with authority in the relevant provisions of the Directive, must lay down more detailed common guidelines for appointing the bodies or public authorities to assist in the verification of whether specific signature-creation devices meet the specified minimum requirements. The Bill also provides authority to implement any joint EU rules thereon or to implement a special Danish regulation thereof where no common guidelines are laid down. It is not directly intended to use the authority in section 15 of the Bill for that purpose until it is clear whether the Commission intends to submit a proposal for common guidelines and, if so, whether agreement has been reached on the contents of such guidelines.

9. A general rule on use of electronic signatures on areas with formal requirements ➦

Danish law does not contain any general rules on the significance of signing a document etc., and there is no general definition of what constitutes a signature. In some areas, however, the legislation does contain provisions with formal requirements - for example, that a document must be signed. The provisions may be formulated in various ways and may for instance be supplemented with a requirement that the authenticity of a signature be verified by an attesting witness. Because of the varied formulation of the provisions, it is not certain that a signature which complies with a signature requirement in one set of rules also complies with a similar requirement in another area of law.

The reason why it has been found necessary to make detailed rules only within a single area of law as regards requirements concerning signatures is probably bound up with the fact that a signature has a firmly established function and is seen as an everyday and familiar action. Furthermore, the means used for making a signature (a pencil, ballpen, etc.) are technically simple, and apart from reading skills no other special knowledge or access to technical aids is needed to read a signature.

There is nothing to prevent the question of what constitutes an electronic signature from being left, in the same way, for regulation in each individual area of law. However, the Government has found it best to introduce a general provision stating that each statutory formal requirement concerning signatures on data messages shall be understood to mean that the requirement can be met by using an electronic signature that complies with some security requirements described in detail.

The need for such a rule is bound up with the fact that Article 5, paragraph 1, of the EC Directive on a Community framework for electronic signatures contains a rule on the legal effects of electronic signatures, which means, among other things, that signatures complying with certain security requirements etc. must be deemed to meet requirements in the Member States' legislation on electronic signatures. Only in the case of communication with public authorities does the Directive (Article 3, paragraph 7) to a limited extent enable Member States to make more stringent requirements.

In other words, with the Directive a kind of European standard for electronic signatures is introduced. If a person sends or receives a signature that complies with the requirements of

the Directive, he should be able to expect it to comply with formal requirements concerning the use of electronic signatures in all EU countries.

Correct implementation of the Directive thus means that Danish legislation must not contain any formal requirement for electronic signatures to comply with more stringent security requirements etc. than what follows from the Directive. This is best ensured by introducing a general rule with the described contents.

Furthermore, it is more complicated to decide what is needed to meet a formal requirement concerning electronic signatures than a requirement concerning traditional signatures. This is because an electronic signature is based on methods that are technically complicated and difficult for most people to understand.

The encryption algorithms on which an electronic signature is based have different security levels - at least at the moment - and are being constantly improved. A signature that is secure today may not be so in five years' time, and some signatures provide only limited security from the outset as to the identity of the signatory because, for example, the identity was only superficially checked in connection with the issuance of the certificate.

Proof that a signature originates from the indicated signatory also depends on a number of circumstances that recipients of a signature have only a limited chance of checking. This applies, for example, to the circumstances in connection with the issuance of a certificate and the security procedures for use of the signature-creation device (PIN codes etc.).

Because of the many different types of signature with different levels of security, a formal requirement concerning use of electronic signatures that can be met by any signature would be largely without content, and it must thus be expected that, in the vast majority of cases, more detailed rules would be needed concerning the requirements to be complied with by an electronic signature in order to meet a specific formal requirement in the legislation. A general provision specifying the content of such formal requirements would facilitate the drafting of legislation for the areas in which it is desired to introduce formal requirements on the use of electronic signatures. It would thus suffice to refer to the proposed general provision instead of specific technical provisions on the requirements to be met by an electronic signature in order to comply with the formal requirement in each and every rule of law.

It is important to emphasise that the proposed provision is of no significance to the question of the areas of law in which electronic communication may be used. The rule will only affect the areas of law in which, according to the applicable rules, it is possible to use electronic communication. Whether electronic communication may be used in a specific area of law depends on whether there are formal requirements that can only be met by the use of paper documents. The Ministry of Justice's committee on the legal effects of digital signatures etc. is currently considering whether a legislative initiative is needed to enable use of electronic communication in all areas where that is possible and expedient.

Article 5 of the Directive also specifies that Member States must ensure that electronic signatures can be used as evidence in legal proceedings. Danish law is based on a principle of freedom to produce evidence, which means that the parties to a lawsuit have the right to produce any (relevant) fact as evidence. Thus, according to Danish law, there is no obstacle to using electronic documents, electronic signatures etc. as evidence in lawsuits, so legislation will not be needed to comply with the Directive's requirement on this matter.

Finally, Article 5, paragraph 2, of the Directive contains a general ban on refusal to give electronic signatures legal effect solely on the grounds that the signature is electronic or

fails to comply with the conditions for being an "advanced electronic signature". It must be assumed that the provision serves as a kind of "discrimination ban", meaning that the Members States must not refuse to give an electronic signature legal effect solely on the grounds that it is in electronic form. Such rules have existed earlier in legal systems in other European countries. However, Danish law does not contain any rules with such content, so legislation will not be needed to comply with the requirement of the Directive on this matter.

F. The economic, administrative, commercial and environmental consequences of the Act ➦

Economic and administrative consequences for the State and local and county authorities ➦

The Bill implies establishment of a regulatory authority for certification authorities wishing to offer qualified certificates. It is suggested that the National Telecom Agency act as this authority. To undertake this task, the National Telecom Agency would need an additional two to three man-years.

The Bill authorises the Minister of Research and Information Technology to lay down rules to the effect that the costs of the regulation must in the long term be financed by the certification authorities involved. However, governmental co-financing of the regulatory scheme is needed so as not to burden the market in the preliminary establishment phase. Apart from that, the Bill is not expected to have any particular economic consequences for the State.

The Bill will improve the possibility of using electronic signatures in practice, also in areas where legally binding transactions are made, and where proof is needed of the use of reliable products (certificates and signatures). Public authorities will be able to offer a number of new electronic functions and services for situations in which they need to be sure who they are communicating with and what they are communicating about. Use of electronic signatures will enable public authorities to offer solutions that enable citizens to get access to electronic self-service facilities via the Internet. In the long term, such use must be expected to reduce the administration resources of the public authorities in question.

Economic and administrative consequences for the business community ➦

Implementation of a regulatory scheme and clear regulation of the liability of certification authorities covered by the scheme may increase confidence in the use of electronic signatures and certificates and thus create a better basis for business activities for the certification authorities.

Access to electronic communication based on common standards and a high security level are expected to give added profit in individual companies due to rationalisation 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.

Environmental consequences ➦

Gradually as the Bill takes effect, it will provide clear benefits for 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 for the

environment.

Administrative consequences for citizens

The improved possibilities of electronic communication with public authorities described above will also mean considerably easier administration for the citizens.

G. Consultation ➦

A draft for this Bill has been circulated for consultation to: [original Danish text]

Advokatsamfundet, Akademikernes Centralorganisation, Amtsrådsforeningen i Danmark, Arbejderbevægelsens Erhvervsråd, Arbejdsløshedskassen for selvstændige erhvervsdrivende i Danmark, Arbejdsmarkedsstyrelsen, Arbejdsministeriet, Arbejdsskadestyrelsen, Beredskabsstyrelsen, Brancheforeningen for telekommunikationsindustrien, Brancheorg. for Forbruger Elektronik, By- og Boligministeriet, Børsmæglerforeningen, Canal Digital Danmark A/S, Center for IT-forskning, Center for Ligebehandling af Handicappede, Center for Menneskerettigheder, Christian Rovsing A/S, Civilretsdirektoratet, Copy-Dan, CSC Datacentralen, Danmarks Aktive Forbrugere (DAF), Danmarks Nationalbank, Danmarks Radio, Danmarks Rederiforening, Danmarks Statistik, Dansk Autoriseret Markedsplads A/S, Dansk BiblioteksCenter A/S, Dansk Blindesamfund, Dansk EDI Råd, Dansk Dataforening, Dansk Ejendomsmæglerforening, Dansk Handel & Service, Dansk Industri, Dansk O.T.C., Dansk Standard, Danske Dagblades Forening, Danske Elværkers Forening, De Samvirkende Invalideorganisationer, Debitel Danmark A/S, Den Sociale Ankestyrelse, Den Sociale Sikringsstyrelse, Det Centrale Handicapråd, Det Danske Handelskammer, Det Kommunale Kartel, Det Kongelige Bibliotek, Direktoratet for Arbejdsløshedsforsikringen, Direktoratet for Arbejdstilsynet, Direktoratet for Kriminalforsorgen, Den Danske Dommerforening, Dommerfuldmægtigforeningen v. Retsassessor Carin Heiner Holm, DSB, Eksport Kredit Fonden, Eksportfremmerådet, Elektronikindustrien, Energistyrelsen, Erhvervs- og Selskabsstyrelsen, Erhvervsfremme Styrelsen, Erhvervsministeriet, EU-direktoratet, FDA v/landsformand Viggo Bækgaard, Finansministeriet, Finansrådet, Finanstilsynet, Folketingets Ombudsmand, Fondsrådet, Forbrugerombudsmanden, Forbrugerrådet, Forbrugerstyrelsen, Foreningen af Interne Revisorer, Foreningen af Internetleverandører, Foreningen af Management Konsulenter, Foreningen af Registrerede Revisorer, Foreningen af Statsautoriserede Revisorer, Foreningen for Dansk Internet Handel, Forsvarsministeriet, Frederiksberg Kommune, Færøernes Landstyre, Global One, GN Store Nord, Grossistforeningen for Radio og Elektronik, Grønlands Hjemmestyre, Handelshøjskolen i København, Håndværksrådet, Indenrigsministeriet, InvesteringsForeningsRådet, IT-Brancheforeningen, ITEK, Justitsministeriet, KODA, Kommunedata, Kommunernes Landsforening, Kongeriet Danmarks Hypotekbank, Konkurrencerådet, Kort & Matrikelstyrelsen, Kulturministeriet, Københavns Fondsbørs A/S, Københavns Kommune, Landsorganisationen i Danmark LO, Leverandørforeningen for Radiokommunikation, Miljø- og Energiministeriet, Mobilix, Multi Medie Foreningen, Næstved Kommune, Patentdirektoratet, Pengeinstitutternes Betalings Service PBS A/S, Plantedirektoratet, Post Danmark, Realkreditrådet, Registertilsynet, Rigspolitichefen, Rigsrevisionen, Ringsted Kommune, Rådet for Dansk Forsikring og Pension, Skatteministeriet, Socialministeriet, Sonofon I/S, Statens Arkiver, Statens Bibliotekstjeneste, Statens Bilinspektion, Statens Information, Statens Luftfartsvæsen, Statsadvokaten for Særlig Økonomisk Kriminalitet, Statsministeriet, Sundhedsministeriet, Sundhedsstyrelsen, SU-styrelsen, Søfartsstyrelsen, Tele Danmark A/S, Tele2 A/S, Telekommunikationsforbundet, Telestyrelsen, Telia A/S, Told- og Skattestyrelsen, Trafikministeriet, Udenrigsministeriet, Udlændingestyrelsen, Undervisningsministeriet, Vordingborg Kommune, Værdipapircentralen, Ældre Sagen, Økonomiministeriet, Økonomistyrelsen, Århus Amt, Advokat Hanne Bender, Professor dr.jur. Jens Peter

Christensen and professor dr. jur. Karsten Revsbech, Århus Universitet, Centerleder Knud Erik Skouby, Danmarks Tekniske Universitet, as well as Professor Mads Bryde Andersen, professor dr. jur. Mogens Koktvedgaard and professor dr. jur. Peter Blume, Københavns Universitet.

H. Table of the consequences of the Bill ➦

Positive consequences/lower costs

Negative consequences/additional costs

Economic consequences for the State and local and county authorities

Lower resource requirements for undertaking various services offered by using electronic communication and electronic signatures.

To undertake the task of regulating certification authorities, the National Telecom Agency would need an additional two to three man-years.

Investments needed in new technology, training of personnel, etc. in connection with the provision of new electronic services.

Administrative consequences for the State and local and county authorities

Better possibility for public authorities to use electronic signatures that comply with a sufficiently high level of security to meet citizens' need for use and protection of personal data in connection with electronic services.

None

Economic and administrative consequences for the business community

Certification authorities offering qualified certificates must pay the cost of a system auditor and of submitting various data to the National Telecom Agency. In the long term it is also intended to lay down rules to the effect that the State's costs in connection with the National Telecom agency's regulatory activities must be paid by the certification authorities.

The introduction of rules on regulation of and liability for certain certification authorities is expected to increase the credibility of electronic signatures and thus to improve the basis of business activities for the certification authorities.

Improved possibility of using and developing electronic commerce, which may result in considerable savings for the business community and improve its competitiveness to foreign companies.

Environmental consequences

As the use of electronic services spreads, it will produce clear environmental benefits because of lower resource requirements for transport of messages, savings in paper consumption, etc.

The Bill has no appreciable negative consequences to the environment.

Administrative consequences for citizens

The improved possibility of communicating electronically with public authorities would mean considerably easier administration for citizens.

No negative administrative consequences for citizens.

Relationship to EU law

The Bill contains rules that implement Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Notes to the individual provisions of the Bill

Part 1. Scope and application ➦

Section 1: The purpose of the Bill is to ensure that there will be products and certification authorities on the market that comply with requirements that make them secure to use.

The Bill thus lays down requirements for certificates offered as "qualified certificates". The providers of such qualified certificates will be subject to a number of minimum requirements, public regulation and a special liability regulation. It is not a question of an actual prior authorisation scheme, but a scheme based on submission of documentation (including, in particular, system auditor reports) of compliance with the minimum requirements, combined with the possibility of suspending a certification authority's right to use the government-regulated product description "qualified certificates" about its product if the documentation is insufficient or the requirements are not complied with. The Bill will thus help to advance secure and efficient use of digital communication.

The purpose of the Bill is not to regulate all offers to provide certificates for electronic signatures. Certification authorities will be able to decide for themselves whether to use the term "qualified certificates" about their products and thus be covered by the Act's regulatory scheme and associated liability provision.

In addition to the above-mentioned, the Bill contains specific regulation of the minimum requirements concerning signature-creation devices, see also the notes on sections 14-15 of the Bill.

Section 2: The provision specifies the application of the Bill.

The Bill will primarily apply to certification authorities established in Denmark and to the qualified certificates that these authorities issue to the public.

The Bill also contains rules on signature-creation and signature-verification data that certification authorities provide in combination with a qualified certificate.

Finally, the Bill lays down a number of requirements for secure signature-creation devices that are marketed and used in Denmark, including that they must basically be verified by a body or authority designated by the Minister of Research and Information Technology.

Subsection (1):

As far as the specific regulation of certification authorities is concerned, the territorial scope of the Bill covers only certification authorities established in Denmark

For a certification authority to be regarded as established in Denmark it must undertake financial activities from a permanent address in Denmark for a non-specified period of time or for a certain period of time.

An example of a certification authority that will undoubtedly be covered by the provisions of this Act, is a company established and registered as a Danish company in accordance with Danish company law, and domiciled in Denmark. Such establishment and registration must be taken to mean that the company is managed in this country and is carrying out its main financial activities here. If such a certification authority chooses to offer its services in another country, it will still have to comply with the provisions of this Act and will still be subject to Danish regulation.

Contrary to this, a certification authority that offers its services on a website on the Internet set up via a Danish Internet provider but does not otherwise undertake activities in Denmark will not be regarded as established in Denmark (i.e. in the country where the Internet provider is located). It does not matter in which countries the website of a certification authority is accessible.

If a certification authority is established in several locations, the decisive factor is the location from which the services in question are supplied. If that is difficult to decide, importance must be attached to where the centre of the certification authority's activities relating to the services in question is located and, ultimately, also where the company's head office is domiciled.

Whether a certification authority must be regarded as being established in Denmark or in another country within the European Economic Area (EEA) is important for deciding which country's authorities etc. are to check that it complies with the requirements for issuing qualified certificates. Article 4, paragraph 1, of the Directive thus introduces a form of work-sharing between the Member States.

A more detailed definition of when a certification authority must be regarded as being established in Denmark or another country must be decided in practice on the basis of an interpretation of the rules contained in the Treaty on European Union regarding the right of freedom of establishment and other relevant EC directives.

In accordance with the requirement in Article 4, paragraph 1, of the principles of the Treaty on European Union on freedom to provide services, the Bill does not impose limitations on certification authorities established in another country within the European Economic Area (EEA) with respect to marketing and issuing certificates on the Danish market. Certification authorities established in EEA countries may, in so far as they comply with the requirements of the Directive, also market and issue certificates termed qualified certificates in Denmark.

Qualified certificates issued by a certification authority established in these countries may be used to meet formal requirements in the legislation, see section 13 of the Bill, in the same way as a qualified certificate issued by a certification authority established in Denmark. This also applies to certificates issued by certification authorities in third countries, provided the conditions stipulated in section 23 are complied with.

Whether a certification authority not established in Denmark meets the Directive's requirements on certification authorities that issue qualified certificates must be checked by

the authority or private body in the country of establishment designated to do so in accordance with the rules of the country in question. Article 3, paragraph 3, of the Directive states that each Member State must ensure the establishment of an "appropriate system that allows for regulation of" certification authorities that are established on its territory and issue qualified certificates to the public. No further requirements are specified as to the scope of such regulation and this may thus vary in extent and detail from one Member State to another.

The Bill applies primarily to the provision of qualified certificates to the public and thus does not regulate the use of electronic signatures and certificates used exclusively within dedicated systems based on voluntary agreements between a specified number of participants. The Directive does not contain any detailed definition of what provision of certificates "to the public" shall be understood to mean, which is why it must be decided in practice how to interpret the expression.

However, in the assessment of concrete cases the critical question is probably whether or not a certificate can be used vis-à-vis third parties with whom the signatory has not made any prior agreement on use or acceptance of the certificate in question.

An example of such a dedicated system not regulated by the Bill would be an Internet banking system where it is only the bank that has to use and accept the signatory's certificate. Similarly, it must be assumed that certificates that can only be used within one or more organisations or companies will not be covered.

The Bill's rules on certification authorities, with the exception of the provisions in section 12, must only apply to certification authorities established in Denmark and which issue qualified certificates. Section 12, however, applies to all certification authorities established in Denmark whether or not they issue qualified certificates or certificates to the public. For the sake of the formulation of the Bill's provisions, the term "certification authority" is used everywhere in the Bill. See also the notes on section 12.

Subsection (2):

The Bill applies also to verification of compliance by signature-creation devices with the specified requirements for secure signature-creation devices. See also the notes on section 15 on the geographic scope of these provisions.

Part 2. Definitions ➦

Part 2 contains the definitions of the terms used in the Bill. The terms originate, inter alia, from the definitions in Article 2 of the Directive, and they form the basis for establishing an internal market for certification services that comply with these requirements.

Section 3:

Subsection (1), 1):

This provision defines what an electronic signature shall be understood to mean. The most widely used electronic signature technology today is the so-called digital signature, which is based on a system with a private and public signature key.

However, the Bill also covers other electronic systems intended to identify users such as codes and biometric values. The Bill is based on a principle of technology-neutral regulation

and thus covers all kinds of electronic methods to establish the authenticity of a message. A method of authentication means a method to check that a message originates from the person indicated as signatory and that the content has not been changed after the electronic signature was attached.

A digital signature works as follows: the signatory has a private signature-generation key, which he uses to create or generate the digital signature. To this private key is attached a public signature-verification key. The private key is used to check the digital signature.

The private and the public key match like two halves of a lock or a code so that a message signed with one of the keys can only be verified with the other.

2):

Point 2) contains a definition of what an advanced electronic signature shall be understood to mean. For an electronic signature to be regarded as an advanced electronic signature it must be able to identify the signatory and be uniquely linked to that person, see points (a) and (b).

With respect to the security of the electronic signature, it is required in point (c) that an advanced electronic signature be based on a signature-creation device using means that the signatory can keep under his sole control.

Point (d) stipulates that an advanced electronic signature must be able to reveal any change made in the signed data after the signature was attached to them. The user must thus be able to see if changes have been made to the signed data after the signature was attached to or logically associated with them.

This definition is used in section 13 of the Bill, which contains the first part of a specific regulation of the legal effects of using electronic signatures.

3):

A definition is given in point 3) of what a signatory shall be understood to mean. The signatory is the person that controls a signature-creation device and holds the signature-creation data (the private key). It is thus the person that appears from the certificate and that has created the signature on the signed data.

4):

Point 4) defines what signature-creation data shall be understood to mean. Signature-creation data are the data used to create the electronic signature. In the digital-signature technology, signature-creation data are called the private key.

5):

Point 5) specifies what a signature-creation device shall be understood to mean. A signature-creation device is the system used to create the electronic signature and is typically based on an encryption algorithm and a decryption algorithm with associated encryption keys. An encryption algorithm is a formalised way of creating an electronic signature. The encryption keys are parameters that are used for the encryption algorithms for practical reasons. The keys decide how the algorithms create the electronic signature.

The signature-creation device uses the signature-creation data. The device can be

software-based as well as hardware-based. A possible hardware solution is when the signature-creation data is stored on a so-called chipcard (a plastic card).

A software-based signature-creation device will typically be contained in the electronic mail system.

Sections 14 and 15 contain further rules on so-called "secure signature-creation devices".

6):

According to point 6), the signature-verification data are the data used to verify the electronic signature, i.e. the public part of the key pair.

7):

The provision in point 7) specifies what a signature-verification device shall be understood to mean. It is a system used to verify the electronic signature.

8):

Point 8) defines a certificate. A certificate for an electronic signature contains information about the signatory. The signatory is the person that holds a signature-creation device and that makes an agreement with a certification authority on the issue of a certificate for the signatory's signature. The certificate is the electronic attestation stating the connection between the identity of the signatory and the latter's signature-verification data (also called the public key in digital signature technology).

9):

Point 9) defines what is considered in the Bill to be a certification authority. The core activity of a certification authority is to verify the identity of the signatory and state the connection between the signatory and his or her signature-verification data in a certificate issued by the certification authority. In addition, certification authorities that issue qualified certificates must ensure the operation of a prompt and secure directory and a secure and immediate revocation service, see section 9.

A certification authority is free to carry out other forms of activities, including a number of related services such as validation and time stamping, and to guarantee certificates issued by other certification authorities, see sections 11 and 23, etc.

The provisions in Part 2 constitute a partial implementation of Article 2 of the Directive, which contains 13 definitions of terms used in the Directive. The provisions in Part 2 implement Article 2, points 1-5, 7-9 and 11, of the Directive. Article 2 (6) is implemented by section 14; Article 2 (10) is implemented in Part 3; and, finally, Article 2 (12) of the Directive is implemented by section 5 (1) point 3). It has not been found necessary to implement the definition of voluntary accreditation in article 2 (13) of the Directive, see also the notes on section 10 (1) point 4).

Part 3. Qualified certificates ➦

Part 3 contains requirements on the provision of "qualified certificates".

Section 4:

Subsection (1):

A qualified certificate is defined in subsection (1) as a certificate which contains the data required in subsections (2) and (3) and which is issued by a certification authority that meets the provisions of Part 4 and rules laid down in pursuance thereof.

The provisions in subsections (2) and (3) are an implementation of the requirements made in the Directive on the provision of "qualified certificates".

If a certificate includes an indication that the certificate is issued as a qualified certificate, and if the issuing certification authority is domiciled in Denmark, then the requirements in this Bill on the provision of qualified certificates must be met.

Certification authorities that do not comply with the provisions of the Act on qualified certificates must not use the designation "qualified certificates" about their certificates or designations that give the impression that qualified certificates are implied.

Subsection (2):

Subsection (2) contains the requirements concerning the data to be contained in a qualified certificate.

According to point 1), it must be indicated in a qualified certificate that it is issued as a qualified certificate.

Point 2) requires a certification authority to state its domicile. This information makes it clear to the person who trusts a certificate which country is regulating the activities of the certification authority in question.

Point 2) also contains a requirement that the certificate must contain an identification of the certification authority. This means that the name of the certification authority in question must appear from the certificate. In most cases the best thing to do is to use the identification that the provider normally gives to the public since that will give the certificate recipients a direct impression of who the issuer is. Other unique identification than the name of the certification authority may be stated, for example the certification authority's tax reg. no. (SE no.), central business reg. no. (CVR no.) or company reg. no., or the formally registered company name if that differs from the name or brand name normally used by the company to address the public.

According to point 3), a qualified certificate must contain the name of the signatory. The name of the signatory can also be in the form of a pseudonym and if that is the case, it must be identified as such.

A decisive factor for trusting an electronic signature is that the identity of the signatory can be directly seen. According to section 6, the certification authority is under an obligation to verify the identity of the person to whom a qualified certificate is issued.

Point 4) specifies that the certificate must contain any other information about the signatory which is needed for use of the certificate. What is considered other relevant information depends on the actual purpose of the certificate, but it could include information that ensures unique identification of the signatory. If, for instance, it is a certificate that will only be used for communication with an insurance company, it might be useful if it contained the signatory's policy number. The Bill does not take a position on whether a qualified

certificate may contain the signatory's civil registration number or similar kind of identification. That will have to be decided under the general law on the handling of personal data.

According to point 5), a qualified certificate must contain an activation and expiry date, i.e. an indication of the beginning and end of the period of validity of the certificate.

This provision allows for the fact that an electronic signature attached to a message will gradually become obsolete as the technology allowing the code to be broken gets faster and more sophisticated. In a few years' time the elements that constitute a secure electronic signature today will no longer provide protection against forgery etc.

When using electronic 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. The problems surrounding obsolete certificates mean that it should be considered specifically whether a given type of messages is suitable for electronic communication.

The provision in point 6) requires any limitations on the scope of use of a certificate (scope limitations) to be stated clearly in the certificate.

The provision in point 7) requires any limits on transaction amounts for which a certificate can be used (amount limitations) to be stated clearly in the certificate.

The provision in point 8) requires a qualified certificate to contain a unique identity code, a so-called reference number. It should thus be possible to uniquely identify a certificate.

Under point 9) it is required that a qualified certificate contain the signature-verification data that correspond to the signatory's signature-creation data.

If a certificate does not contain the above-mentioned data, it will not be possible directly to verify the electronic signature. The signature can only be verified when the signature-verification data have been collected from the certification authority. This might keep certain users from verifying the signature, with a consequent lack of security. That is why a qualified certificate must contain the signature-verification data so that a signature can be directly verified.

Subsection (3):

According to subsection (3), a qualified certificate must be signed with the advanced electronic signature of the certification authority. The signature is attached to or logically associated with the certificate after all the data have been inserted. This will ensure that a certificate cannot be changed after it has been issued without this being detected and the recipient thus warned.

The signature of the certification authority and the identification of the authority in the certificate, see subsection (2), point 2), will serve to identify to whom a claim for compensation under section 11 can be addressed.

Part 4. Requirements concerning the activities of certification authorities ➦

Section 5:

Subsection (1):

The provision requires certification authorities that provide qualified certificates to take the measures needed on a current basis to ensure that they will have a secure, reliable and well-functioning offering of qualified certificates. What such necessary measures are will have to be decided on the basis of the services provided and the potential customers. A certification authority is under an obligation regularly to assess its measures if its portfolio of services offered is extended or in other ways changed.

Point 1) requires a certification authority to follow the standards for administrative and management procedures recognised for the technology within which the provider offers its services.

Point 2) stipulates that certification authorities issuing qualified certificates must employ personnel that possess the required expert knowledge, experience and qualifications for the services provided. The requirements may differ from one service provider to another depending on the services provided.

The personnel must possess expertise in electronic signature technology and be familiar with proper security procedures. Certification authorities must do all they can to ensure that any breach of security is not due to personnel-related factors.

Point 3) obliges certification authorities that issue qualified certificates to use secure IT products and systems for their activities. Among other things, certification authorities must use systems and products that are protected against unauthorised modification.

It is vital for the security of the infrastructure built up around the electronic signatures that the certification authority, which has to appear as a trustworthy third party, use reliable systems and products and that the systems and products applied are designed in such a way that the security surrounding the activities of the certification authority is optimal.

Point 4) requires certification authorities to take measures and establish procedures against any possible forgery of certificates. The provision is intended to ensure that certificates are not falsified after they have been issued. The integrity of a certificate can be secured, for example, by the certification authority attaching its own electronic signature to the certificate. See section 4, subsection (3).

According to point 5), certification authorities that issue qualified certificates are required to maintain sufficient financial resources at all times to meet the requirements of this Act, including in particular the ability to honour any liability for damages.

Whether a certification authority has sufficient financial resources will depend, among other things, on the services offered by it. This means that, if a certification authority offers certification services for use within an area of high economic risk for the parties involved, then the financial resources must be equally large. The certification authority must thus maintain the right balance between its financial resources and the extent and nature of the activities performed. The certification authority can meet the requirement by, for example, obtaining appropriate insurance. Subsection (3) authorises the Minister of Research and Information Technology to lay down more detailed rules on the financial resources of certification authorities, including requirements for certification authorities to take out an insurance when deemed necessary, and to lay down detailed rules on such insurance.

Points 3) to 5) implement Annex II, points (f) to (h), of the Directive.

Section 5 (1), points 1) and 2), lay down requirements that implement Annex II, points (a) and (e), of the Directive.

Subsection (2):

Subsection (2) stipulates that certification authorities issuing qualified certificates must appoint an external state-authorised public accountant to carry out their internal system audits. The provision is a minimum provision in the sense that if Danish company law, the Danish Company Accounts Act, or any other law, stipulates that a certification authority must have one or more financial auditors, then these rules must also apply to the certification authority. The provisions of the Bill only apply to the use of external auditors necessary to comply with the rules of this Act.

The requirement that certification authorities must have a system auditor is based on the specific requirements made in this Bill for certification authorities providing qualified certificates. These requirements mainly concern certification authorities' IT systems and the related security.

In this Bill, system auditing means auditing of 1) general computer control routines in the company, 2) computer-based user systems for issuing, verifying, storing and revoking certificates, and 3) computer systems for exchange of data with others. In connection with his audit, the appointed system auditor must judge whether the certification authority complies with the provisions of this Act and the rules laid down in pursuance thereof.

Auditing of general computer control routines includes verification by the appointed system auditor of the general security measures to establish a state-of-the-art IT security level at the certification authority. Auditing of computer-based user systems covers computer-based as well as manual procedures.

The costs incurred by the appointed system auditor will be paid by the individual certification authority.

See also the notes on section 17, including section 17, subsection (4), which gives authority to lay down detailed rules on how to carry out system auditing and on the qualifications of system auditors.

Subsection (3):

Subsection (3) authorises the Minister of Research and Information Technology to lay down detailed rules on the content of the requirements given in subsection (1) concerning certification authorities that issue qualified certificates to the public.

Article 9 of the Directive makes it possible for the Commission to clarify the requirements laid down in the Annexes to the Directive on the provision of qualified certificates. The authority given in subsection (3) can be used to implement this, but also to lay down specific Danish rules thereon. The intention is to lay down detailed rules on the minimum requirements concerning the financial resources of certification authorities and/or insurance matters, see also the notes above on subsection (1).

Section 6:

According to section 6, certification authorities must specify and apply adequate procedures for verifying the identity and other facts concerning the signatory prior to the issuance of a

qualified certificate.

The provision does not prevent certification authorities from appointing another organisation, a so-called registration authority, to carry out the required identity check.

However, it will still be the certification authority which, under section 11 of the Bill, is responsible for the data in the certificate being correct. It thus makes no difference to the signatory of a qualified certificate or to a third party who reasonably relies on a qualified certificate whether a mistake in connection with an identity check can be attributed to the certification authority itself or to a registration authority appointed by the certification authority. If a certification authority has had to pay compensation under section 11 due to a mistake made by the registration authority, it may subsequently claim indemnification from the registration authority under the general rules of Danish law on damages.

In pursuance of the authority given in subsection (3), more detailed minimum requirements will be laid down on the types of verification procedures that must be deemed to meet the requirements concerning the performance of a satisfactory identity check.

The most secure method of checking the identity of the person to whom a certificate is issued is to demand that he or she come forward personally and produce relevant photographic identification. It is already common practice, and regulation is in place for it, to set up bank accounts and issue credit cards and payment cards etc. without personal appearance, provided adequate written documentation is submitted and certain prescribed control procedures are used. In a number of situations, there seems to be no reason to make more stringent requirements for issuing an electronic signature certificate than for a payment card. However, which procedures to deem adequate will also depend on what the qualified certificates are going to be used for.

The detailed rules on minimum requirements for identity checks will be based on the above and after consulting all relevant parties. The rules might possibly include differentiated regulation of various categories of certificates.

In this connection, consideration will include the fact that it is ultimately the certification authority that will be responsible for the information in a certificate being correct, see section 11 of the Bill; and there will therefore be a powerful commercial incentive for the certification authority to establish adequate procedures for checking the identity of the parties to whom it issues certificates, since, basically, it will be the certification authority that is held liable if the information in a certificate is incorrect and the recipient of the certificate for that reason suffers a loss, for instance because he is not contracting with the party he believes to be contracting with on the basis of the information in the certificate. So there might be situations in which a certification authority decides to use more thorough control procedures than required by the statutory regulation in order to minimise its own risk.

Consideration will also be given to the fact that a requirement for personal appearance whenever a qualified certificate is issued will probably impede the use of electronic signatures and associated qualified certificates to an unreasonable extent.

In any case, the rules will be formulated such that, in practice, it will be possible to delegate the actual identity check to third parties or to let third parties guarantee the identity of the signatory, although still under the responsibility of the certification authority, see above. So there might be situations in which the identity of the person to whom a qualified certificate is to be issued could be more appropriately checked by a third party. If, for example, a company or public authority wants to issue certificates to all its employees, it will already have sufficient information about them to issue a certificate to each without any need for them to appear in person for registration at the certification authority.

Subsection (2) also requires certification authorities to inform anyone wishing to know how the identity was checked. It is important for the recipient to be able to judge whether the checking done by the certification authority complies with the security level he requires.

The requirement that a certification authority must verify the identity of the signatory of a certificate implements Annex II, point (d), of the Directive.

Section 7:

Subsection (1):

Subsection (1) requires certification authorities that issue qualified certificates to ensure that the signatory, at the time of issuance, holds the signature-creation data corresponding to the certified signature-verification data. Together with section 11, subsection (1) implements Article 6, paragraph 1(b) of the Directive.

Subsection (2):

Subsection (2) establishes that a certificate can be issued by the signatory of the electronic signature himself generating the signature-generating data and signature-verification data to be certified.

The certification authority can also issue a chipcard on which the electronic signature is stored. In such cases the signature-generation data are usually generated by the certification authority.

If it is the certification authority that generates the signature-creation data, then the certification authority must ensure confidentiality of the data during the process of generation. The certification authority also has a duty to ensure that only uniquely linked signature-creation and signature-verification data are used.

Subsection (2) must be read together with section 11 and implements Article 6, paragraph 1(c) and (g), of the Directive.

Subsection (3):

A certification authority must establish a procedure for issuing certificates that makes it possible to determine the date and time of issuance later. In the event of a dispute, it may be important to be able to establish whether and when a certificate was issued. The provision implements Annex II, point (c), of the Directive.

Section 8:

Section 8 requires certification authorities that issue qualified certificates to submit, as a basis for any customer relationship aimed at the issuance of a qualified certificate, a written description of the specific terms of contract for the issuance and any terms and conditions specified for use of the qualified certificate by the certification authority.

The certification authority has a duty to submit all the data needed to enable the customer to assess the terms and conditions and the cost of using the qualified certificate. This is to enable the customer to assess advantages and disadvantages of the certificate in question compared with other certificates.

Subsection (1):

Point (1) requires a certification authority to provide information about the terms and conditions for use of an issued qualified certificate.

Before entering into an agreement on the issuance of a qualified certificate, the certification authority must state whether any limitations on the scope or amounts have been specified. The certification authority may also lay down conditions for use of specific security equipment etc. by the signatory. It must be stated if such conditions are imposed.

In pursuance of point 2), the certification authority can make requirements as to how the signatory must store and protect the signature-creation data attached to the certificate.

The certification authority will thus be entitled to make the issuance of a qualified certificate conditional upon the signature-creation data being stored on a chipcard. It will also be entitled to require the electronic signature to be protected by a PIN code etc.

According to point 3), conditions must be established for the cost of obtaining and using the certificate, and of using other of the certification authority's services.

Point 4) requires the certification authority to provide information about any voluntary accreditation schemes to which it is accredited.

Accreditation scheme means any scheme where a licence is granted which sets out rights and obligations specific to the provision of certification services, and which, upon request by the certification authority concerned, is assigned to the authority by a public or private body charged with the preparation of, and checking of compliance with, such rights and obligations, and where the certification authority is not entitled to exercise the rights given by the licence until it has received the decision of the body in question.

The importance of a certification authority being accredited to a voluntary accreditation scheme is not that the requirements in such a scheme take priority over the provisions of this Act on the provision of qualified certificates. The certification authority still has to comply with the provisions of this Act.

What a voluntary accreditation scheme can do is to ensure provision of services at a more advanced level. If several certification authorities join the same accreditation scheme, it may mean that their certificates can be used in the same situations.

Information about being accredited under an accreditation scheme might influence a customer's choice of certification centre.

According to point 5), terms and conditions for settling disputes and complaints must be established. The sector could set up an independent body to handle complaints about the treatment given by a certification authority.

Subsection (2):

Subsection (2) ensures that the information required under subsection (1) can be submitted electronically, provided it is done using a protocol directly identifiable to the recipient and thus legible. The message must also be given in such a way that it is possible later to prove the conditions under which the contract was concluded.

It will not suffice for the certification authority to refer to a website giving information about the data to be submitted prior to the conclusion of the contract. A website is controlled by the certification authority, which can thus change the terms and conditions at any time with little or no possibility of others being able to prove the terms and conditions applied at the time of issuance.

Section 8 lays down requirements that implement Annex II (k) of the Directive.

Section 9:

Subsection (1):

Subsection (1) requires certification authorities that issue qualified certificates to ensure the establishment of a prompt and secure directory and a secure and immediate revocation service for the certificates issued by the certification authority.

The service must enable checking of whether a qualified certificate is revoked, the validity period of the certificate, or whether the certificate contains any limitations on the scope or amounts. The data must enable the recipient of a certificate to assess whether the certificate is valid and whether it has been used within any limitations specified for use of the certificate.

Section 11 also imposes on the certification authority increased liability for the data in the directory and revocation service being correct and comprising the data required in the provision.

The provision does not prevent a certification authority from making an agreement with another certification authority or another company to provide the service. However, the certification authority continues to be liable under section 11 for any losses incurred in relation to the service.

Subsection (2):

Under subsection (2), the certification authority is required to revoke a qualified certificate immediately upon receipt of such a request from the signatory. Revocation means that the certification authority registers the signatory's wish to have the certificate revoked and that this information is made publicly available, see subsection (1).

The provision must also be seen in connection with the liability provision in section 11 that subjects the certification authorities to a presumption of negligence for failure to meet a request for revocation, etc.

Subsection (3):

Subsection (3) requires that users must have immediate access to the information.

The provision implements the requirements in Annex II (b) and (k) of the Directive. The provision in section 11 extends the scope of the requirements concerning the information that the certification authority must make available in connection with the directory and revocation service compared with what is required in the Directive. The reason for this extension is to increase user-friendliness and thus the security of using qualified certificates.

Subsection (4):

Subsection (4) prohibits registration of a qualified certificate in a publicly accessible database without the explicit consent of the signatory.

A major advantage of the electronic signature is that a user can communicate securely with persons he has not communicated with before, let alone made a communication agreement with.

One way of doing this is to obtain the certificate of the future recipient from a public database. That would provide an incentive to set up such databases. However, as mentioned, the certification authority cannot register a qualified certificate in such a database until it has the consent of the signatory. The prohibition is an implementation of Annex II (l), 3rd point, of the Directive.

Subsection (5):

The provision authorises the Minister of Research and Information Technology to lay down detailed rules on the requirements in subsections (1) to (3).

More detailed rules can thus be laid down on the obligation of the certification authorities to effect revocation immediately upon receipt of a request for this from the signatory and the procedures to be used in such cases, and on their obligation to ensure signatories simple and effective means of contacting them directly, and on their obligation to immediately confirm receipt of such a request so that the signatory can be sure that the request has been received, etc.

Section 10:

Subsection (1):

Subsection (1) requires certification authorities that issue qualified certificates to record and store all relevant information concerning the certificates for at least six years. This is necessary in case evidence of certification is needed in legal proceedings. The provision implements Annex II, point (i), of the Directive.

The requirement that all relevant information must be stored for at least six years, is set out on the basis of the requirements in the Bookkeeping Act for storing bookkeeping material and on the rules of limitations in the 1908 Act with the addition of one year, corresponding to the current accounting period.

The provision does not prevent certification authorities from concluding agreements with signatories for all relevant information to be stored for longer periods of time. This might be particularly relevant in the case of contractual relations expected to run for long periods of time.

The information can be recorded electronically, in which case it must be adequately secured.

Subsection (2):

Subsection (2) requires certification authorities that issue qualified certificates to use trustworthy systems to store certificates in verifiable form. This means that it must be

possible subsequently to verify the content of a certificate. It must be ensured that only authorised persons can make entries and changes in the certificate. If the security of the content of a certificate, and the information about revocation, can be changed by anyone in the certification authority's organisation or no clear guidelines have been set on how such changes can be made and by whom, it might affect the trustworthiness of the electronic signature.

If and when technical changes are made in a certification authority's electronic signature products that might compromise the security of its systems, the changes must be apparent to the personnel using the systems at the certification authority. An example of such products is a software or hardware product used by a certification authority for providing services in connection with electronic signatures or in connection with the creation or verification of an electronic signature. It must be ensured that the personnel operating the certification authority's products and systems are told that actions performed can compromise security.

Thus it is not on every technical change that attention needs to be called to the risk of compromising security. It is only changes which mean that the authenticity of a certificate cannot be checked, or that certificates are made publicly available without the signatory's explicit consent, or that persons not authorised to make changes in the certificates can do so.

The provision thus obliges certification authorities to secure the systems they use by using the best technology available at any time.

Subsection (3):

Subsection (3) prohibits certification authorities that issue qualified certificates from storing or copying the signature-creation data of the persons to whom they have issued certificates.

Storing and copying signature-creation data could cause a serious threat to legal recognition of electronic signatures. It should be ensured that only the signatory has access to the signature-creation data and is thus the only person who has been able to use the electronic signature.

The provision implements Annex II, point (j), of the Directive.

Part 5. Liability ➦

Section 11:

Subsection (1):

The provision lays down the liability rules applying to certification authorities that issue qualified certificates or guarantee such certificates to the public. A Danish certification authority may guarantee to the public that the certificates of another certification authority, including those of a foreign certification authority, comply with the rules for issuance of qualified certificates, see subsection (1).

The certification authority will be liable to pay compensation for losses caused to a person who reasonably relies on a certificate, meaning both the recipient and the signatory of an electronic signature with an attached certificate. A certification authority might also be liable to pay compensation for losses caused to a third party due to negligence by the certification

authority.

The provision does not concern the relationship between the sender and the recipient of a qualified certificate.

According to point 1), the certification authority is responsible for all information in a certificate being correct. This means, for example, that the relevant information about the identity of the signatory must be correct, see also the note on section 6 of the Bill.

According to point 2), a certification authority is liable for losses arising because a qualified certificate did not contain all information required under section 4.

According to point 3), a certification authority is liable for losses caused by failure to revoke a certificate immediately upon receipt of such a request, see section 9, subsection (2).

According to point 4), a certification authority is liable for losses caused by lack of or erroneous information on whether a certificate has been revoked. A certification authority is also liable for losses caused by lack of information about the expiry of a certificate or lack of information about limitations on the scope or amounts, see section 9, subsections (1) and (3).

Point 5) states that a certification authority will be liable for losses caused by failure to comply with the security regulations given in section 7.

Subsection (2):

Section 11 aims to protect consumers in that the provision prescribes fault liability with reversed burden of proof. A certification authority thus has to prove that it has not acted negligently or wilfully.

The reason for implementing increased liability for certain certification authorities is the highly technical and complicated nature of the area. It would be difficult for the general user of electronic signatures without any real knowledge of the technology to prove that a certification authority has made mistakes or acted negligently to an extent that may be deemed culpable or wilful.

The provision was formulated in accordance with similar rules on presumption of negligence in other laws.

Imposing increased liability may help to ensure the required confidence in, and thus an increased use of qualified certificates.

In order to impose on a certification authority liability for losses suffered by the signatory or third party under this provision, the other conditions of the general law of damages must also be met.

Subsection (3):

Subsection (3) exempts a certification authority from liability for losses occurring as a result of use of a qualified certificate outside the limitations applying to the certificate. If a certificate is used outside the scope and amounts limitations on the certificate, a certification authority will not be liable for losses occurring as a result thereof.

For a certification authority to avoid liability under subsections (1) and (2), the limitations must appear clearly from the certificate, see section 4, and information about them must be given on request by the certification authority's directory and revocation service, see section 9, subsections (1) and (3).

Subsection (4):

Subsection (4) states that it must not be possible to depart from the special liability under subsections (1) - (3) by prior agreement.

Subsection (5):

The provision in subsection (5) establishes that, if a qualified certificate is used in situations covered by this Bill and by the rules in the Bill on certain types of legal tender, which is now being dealt with the Folketing, then this Act will only apply if the loss is not covered by sections 10 and 11 of the Act on certain types of legal tender.

The provision is intended to ensure that matters covered both by the Act on certain types of legal tender and by this Bill are judged in accordance with the most stringent set of rules. "Injured parties" thus have the best possible chance of recovering their losses.

If a qualified certificate on a so-called "multi-application card" - i.e. a card used both as a means of payment and for other purposes - is used in situations not covered by the Act on certain types of legal tender, then any possible liability of a certification authority must be judged in accordance with section 11 of this Bill.

Section 11, subsection (1), points 1) and 2), implement Article 6, paragraph 1(a), of the Directive. Subsection (2), point 3), implements Article 6, paragraph 2, of the Directive. However, the provision extends the liability also to cover lack of information on the expiry of a certificate and on limitations on its use.

With reference to section 7 in section 11, subsection (2), point 4), of the Bill, Article 6, paragraph 1(b) and (c), of the Directive are implemented, under which a certification authority is liable for losses arising because the person identified in a certificate did not, at the time of the issuance of the certificate, hold the signature-creation data corresponding to the signature-verification data given in the certificate. A certification authority will also be liable if the signature-creation data and the signature-verification data cannot be used in a complementary manner in cases where the certification authority has generated both of them, see section 11, subsection (2), point 4), together with section 7, subsection (2).

The provisions of section 11 include particularly stringent liability for certification authorities in certain specified situations. Outside these situations the general compensation rules of Danish law apply.

Section 11 does not regulate questions on whether or not a certification authority can claim indemnification from others for compensation paid in pursuance of section 11.

Part 6

Supplementary requirements concerning the processing of personal data

Part 6 applies to all certification authorities established in Denmark whether or not they issue qualified certificates or certificates to the public.

Section 12:

The provision regulates the right to process personal data in connection with the certification authority activities covered by this Act.

The provision applies to all certification authorities established in Denmark, see also the notes on section 2.

The provision applies both to collection of personal data in connection with the issuance of a certificate and the subsequent maintenance of the certificate.

The rules in the Bill on data protection now introduced will also apply to the variations following from this provision.

According to subsection (1), a certification authority may only collect personal data insofar as the data are needed for the purposes of issuing and maintaining a certificate. The data may only be collected directly from the person in question, who will normally be the same as the signatory, unless the latter has given his explicit consent for the data to be collected from other parties as well. The expression "explicit consent" shall be understood in accordance with section 3, point 8), together with section 6 (1), point 1), in the Act on Data Protection.

Subsection (2) states that certification authorities may only process and pass on personal data collected in accordance with subsection (1) for other purposes than issuing and maintaining a certificate provided the person in question has given his explicit consent.

The National Telecom Agency checks compliance with the provision, see section 18, and may in that connection issue an order to a certification authority to comply with the provision, and may impose daily penalties.

The provision implements Article 8 of the Directive.

Part 7. Electronic signature and formal requirements ➦

Section 13:

The proposed provision contains a so-called "rule of judicial implication", the purpose of which is to give certain formal requirements in rules of law in other legislation a specific content. These are rules of law involving a requirement for an electronic message to be provided with a signature or the like. It follows from the provision that such requirements must be regarded as satisfied if an electronic signature that complies with certain security requirements is used, because the signature is an advanced electronic signature, see section 3 (1), point 2), which is also based on a qualified certificate, see section 4, and has been created by a secure signature-creation device, see sections 14 and 15.

The provision only applies to signature requirements etc. that can be met by using an electronic signature and is therefore of no significance to the question of when that is the case. At present, Danish law does not include any rules requiring the use of electronic signatures. However, there are a number of rules of law that contain a signature requirement.

Whether such a formal requirement can be met by using an electronic signature must, as before, be decided in accordance with the rules applying in the relevant area of law.

However, if the result of an interpretation of these rules is that the requirement can be met by using an electronic signature, it follows from the proposed provision that a message provided with an advanced electronic signature that complies with the above-mentioned requirements cannot be rejected or denied effect on the grounds that it does not comply with the signature requirement in question.

Other terms and conditions can be attached to a formal requirement for signatures etc. Compliance with such a formal requirement will often presuppose that the signature originates from and thus identifies a specific person. An electronic signature will often be attached to a specific person, but certificates can also be issued under a pseudonym, see section 4 (2), point 3), and a certificate can also identify a legal person (a company, an association, a foundation, etc.), but not the person who provides the signature for the legal person. The proposed provision only affects the question of what is required to comply with a requirement for a message to be provided with a signature or the like. The provision does not regulate whether a signature can be used with a pseudonym to comply with such a formal requirement.

The proposed provision implies that basically more stringent requirements than those following from the rules in this Act on advanced electronic signatures, qualified certificates and secure signature-creation devices cannot be made in order to regard a signature requirement as met by use of an electronic signature. Therefore, basically, Article 5, paragraph 1(a), of the Directive, which this provision aims to implement, does not open up the possibility of making such stringent requirements.

However, it will be possible to make more stringent requirements for electronic messages to and from public authorities. This follows from Article 3, paragraph 7, of the Directive, which includes a limited exemption on this. In that case, such requirements must be objective, transparent, proportionate and non-discriminatory.

As for the possibility of complying with the requirements of this provision by means of a qualified certificate issued by a certification authority established outside Denmark, reference is made to the notes on sections 2 and 23.

Part 8. Secure signature-creation devices ➦

Section 14:

Subsections (1) and (2):

Subsections (1) and (2) contain the requirements to be met by a signature-creation device, see the definition thereof in Article 3, point 5), in order to be described as a secure signature-creation device. The requirements correspond to the content of Annex III of the Directive.

Whether an electronic signature is created by using a secure signature-creation device is of significance to the legal effects that can be attributed to the signature, see the notes on section 13.

Subsection (3):

The provision implements Article 3, paragraph 5(2), of the Directive, which requires Member States to presume that signature-creation devices that meet generally recognised standards for such devices laid down by the Commission and published in the Official Journal in accordance with the procedure prescribed by Article 9 of Directive comply with

the requirements for secure signature-creation devices, see Annex III of the Directive.

It is not known when the Commission will be able to formulate and publish such standards.

The provision completes the more general requirements laid down in pursuance of subsection (1), in that a company wishing to develop a secure signature-creation device can adapt the device so that it complies with the published standards and thus be sure of having it verified successfully.

The provision may contribute towards the creation of an internal market for secure signature-creation devices and should be read together with section 15 (3).

Section 15:

Subsection (1):

Subsection (1) authorises the Minister of Research and Information Technology to designate one or more appropriate bodies or authorities to assist in verifying that signature-creation devices comply with the requirements stipulated for secure signature-creation devices, see section 14.

The provision allows for a private body to be designated to undertake such verification.

The possibility of having a signature-creation device verified by a body or authority designated under subsection (1) applies not only to providers of such devices established in Denmark but also to certification authorities established in another country within the European Economic Areas (EEA).

The provision also authorises the Minister of Research and Information Technology to lay down rules on the specific procedures for such verification. These may cover actual checking of whether the device meets the requirements of section 14, subsections (1) and (2), and various degrees of self-declaration in accordance with pre-established procedures and in cooperation with an authorised body, as is known from the regulation of radio and telecommunication equipment.

In pursuance of Article 3 (4) of the Directive, the Commission must establish a number of criteria for Member States to determine whether a body or authority is suitable for verifying signature-creation devices.

The authority given in subsection (1) will probably not be used until the Commission has established such criteria, after which it will be possible to set the administrative framework for establishing one or more verification bodies, see also the general notes.

It is assumed that costs associated with checking whether a signature-creation device meets the requirements in section 14, subsections (1) and (2) will be paid by the manufacturers of the systems in question. Rules on this can be laid down in pursuance of the authority given in section 15 (1).

Subsection (2):

For a signature-creation device to be regarded as secure, it must be verified that it complies with the minimum requirements in section 14 of the Act. Verification must be carried out in accordance with the rules laid down in subsection (1).

The designation "secure signature-creation device" may thus only be used when verification as described in subsection (1) has taken place.

Subsection (3):

Subsection (3) states that a secure signature-creation device that has been verified by a body or authority designated in another EEA country, does not have to be verified in accordance with subsection (1) in order to be marketed or used in connection with advanced electronic signatures in the Danish market.

The provision implements Article 3, paragraph 4 (2), and Article 4, paragraph 2.

Similarly, it will be possible to market and use signature-creation devices verified in accordance with subsection (1) in other EEA countries without any need for having them verified in those countries. It will thus be possible to establish an internal market for signature-creation devices.

Part 9. Supervision etc. ➦

The provisions in Part 9 implement the requirement in Article 3 (3) of the Directive that Member States must ensure that providers of qualified certificates are regulated. The regulation also covers compliance with section 12, which sets out requirements for all certification authorities established in Denmark.

Section 16:

Subsection (1):

Certification authorities that issue qualified certificates must comply with a number of requirements laid down in Part 4, and with the provisions laid down in pursuance thereof.

To ensure that the National Telecom Agency is informed about the existence of a new certification authority in the Danish market, it is laid down that the certification authority must notify the National Telecom Agency before, or as soon as, they begin issuing qualified certificates.

In this way, the National Telecom Agency will have a better picture of the companies in the Danish market and be able to check from the start whether the company and its services comply with the requirements of the Act.

It follows from the provision in section 2 that the requirement to notify the National Telecom Agency applies only to certification authorities established in Denmark that issue certificates to the public.

This does not mean that a certification authority has to be authorised or approved by the National Telecom Agency in order to start its activities. Such a requirement would conflict with Article 3 (1) of the Directive, which prohibits Member States from requiring prior authorisation of certification authorities as a condition for carrying out business.

Failure to comply with the notification requirement in subsection (1) does not mean that a certification authority can be prohibited from operating as a certification authority. The National Telecom Agency may order a certification authority to undertake notification, and may impose daily penalties for failure to do so. The National Telecom Agency may also, in

exceptional cases, order a provider not to describe his certificates as qualified certificates, see section 18 (6).

Subsection (2):

Subsection (2) specifies the information that a certification authority must submit to the National Telecom Agency in connection with the notification. This information will serve as general briefing for the National Telecom Agency about the certification authority. A certification authority that issues qualified certificates is not required to be organised in a specific corporate form.

Subsection (3):

Subsection (3) states that a certification authority must report any change of name, domicile, corporate form, if relevant, management and system auditors to the National Telecom Agency not later than eight days after the change has taken place.

Subsection (4):

The provision authorises the National Telecom Agency to lay down detailed rules on any information to be submitted by a certification authority in addition to those specified in subsection (2).

Section 17:

As mentioned in the introductory provisions and in the notes on sections 5 and 18, the idea is that the regulation by the National Telecom Agency of certification authorities that issue qualified certificates must be based to a great extent on a report prepared by the system auditors appointed by the certification authority.

The report must enable the National Telecom Agency to judge whether there are matters indicating that it should use its recourses in pursuance of the Act by requiring a certification authority to submit further information or even to take action against a certification authority by issuing orders, imposing daily penalties or, if that is the case, by depriving a certification authority of its right to use the designation qualified certificates about the certificates it issues.

Subsection (1):

In pursuance of subsection (1), a certification authority must submit a report to the National Telecom Agency while at the same time making a notification in pursuance of section 16. The report will provide the National Telecom Agency with a basis for judging whether the certification authority complies with the statutory requirements for certification authorities that issue qualified certificates.

Subsection (2):

According to point 1), the report must contain a description of the certification authority's activities and the systems used. The description must show, in particular, how compliance with the requirements in Part 4 concerning the certification authority is specifically ensured.

Secondly, according to point 2), the management of the certification authority must declare whether its overall data, systems and operation security are regarded as adequate and in

compliance with Part 4 and the rules laid down in pursuance thereof.

In this connection, "the management of the certification authority" means the board of directors, the management in companies without a board, or similar executive body, depending on how it is organised. The management's declaration to the National Telecom Agency, together with a similar declaration from the appointed system auditor, show whether a certification authority has the required business and security procedures etc. to enable it to comply with the requirements of Part 4 of the Act and the provisions laid down in pursuance thereof.

Point 3) states requirements to the effect that the appointed system auditor must declare separately that the certification authority's overall data, system and operation security must be regarded as adequate and in compliance with Part 4 and the rules laid down in pursuance thereof.

The reason for requiring both the management of the certification authority and the appointed system auditor to submit a declaration in connection with the report to be submitted to the National Telecom Agency is to get two independent assessments of whether the certification authority complies with the Act. The company's management is responsible for constant compliance with the requirements of the Act and must be expected to know most about any problems in that respect. It must be assumed that the appointed system auditor also has thorough knowledge of the activities of the certification authority besides expert knowledge of auditing, documentation, etc.

Subsection (3):

Subsection (3) requires certification authorities to prepare an updated report each year on their compliance with the statutory requirements.

The report and declarations must be submitted to the National Telecom Agency within a deadline set by the National Telecom Agency. The National Telecom Agency will also determine the period of time to be covered by the report. Basically, to ensure that the information received is not outdated, the submission deadline should be not more than three months after the period covered.

The National Telecom Agency may prescribe different submission deadlines for reports from the individual certification authorities in order to avoid all reports being submitted at the same time. This would ensure better utilisation of the Agency's resources. At the same time, account can be taken of the individual certification authorities, which may use different financial years, etc.

It is assumed that the date for submission of the individual certification authorities' annual report cannot be changed in the subsequent years, unless special reasons speak in favour of this.

The updated report and the declarations from the management and appointed system auditor are important tools for the National Telecom Agency's regular checking of whether a certification authority meets the requirements of the Act.

Subsection (4):

Subsection (4) authorises the National Telecom Agency to lay down detailed rules on the content of the first report to be submitted to the Agency in connection with the notification by the certification authority and the subsequent yearly reports; on the declarations to be

submitted by the management and the appointed system auditor, and on how the system auditing is to be carried out at the certification authorities that issue qualified certificates.

The authority enables specification of more precise requirements for the content of documentation, so that the content of the documentation from the various certification authorities is comparable and enables definition of the type of information deemed necessary by the National Telecom Agency in order to carry out its tasks in accordance with the Act.

More detailed requirements can also be laid down on the content of the declarations to be submitted by the management and the appointed system auditor to the National Telecom Agency.

Finally, the National Telecom Agency is authorised to specify the general framework for carrying out system audits at certification authorities, including, among other things, requirements on the scope of the system audits, the working conditions for the system auditors, their access to take part in management meetings, preparation of a specific audit protocol, cooperation with internal auditors at certification authorities, where applicable, requirements concerning the qualifications of system auditors, etc.

Section 18:

Subsection (1):

The National Telecom Agency is appointed to maintain general supervision to ensure compliance with the Act.

The National Telecom Agency must check that the requirements of the Act both on certification authorities and on the certificates they issue are complied with. The requirement that certification authorities issuing qualified certificates be subject to governmental regulation is intended to ensure that certification authorities using the designation qualified certificates about the certificates they issue have a quality and security level in which users can have confidence.

The National Telecom Agency will undertake only limited regulation of certification authorities that do not wish to issue qualified certificates. With the exception of section 12, the rules of the Act will not apply to these enterprises. These certification authorities will be able to establish themselves freely and operate in accordance with quality requirements and standards that prevail in the market.

Unlike the regulation of companies in the financial sector today, it is not intended that the National Telecom Agency should actually inspect the companies subject to regulation.

The main task of the National Telecom Agency will be to assess the reports to be prepared and submitted by certification authorities when they start operating, and after that once a year.

If the information that the National Telecom Agency receives from a certification authority, its auditors, users or others causes doubt about whether the certification authority complies with the requirements of the Act, the National Telecom Agency will apply the recourses provided for in the Act.

The provision also specifies the detailed rules on the National Telecom Agency's powers to

make decisions regarding certification authorities that issue qualified certificates. The Agency may issue orders, impose daily penalties and deprive a certification authority of its right to designate certificates as qualified certificates.

There may be cases where a certification authority is also subject to other regulatory schemes, for example in the financial sector. This is not regulated by this provision. However, it is assumed that the National Telecom Agency and the relevant supervisory authorities will cooperate to the extent needed to avoid unnecessary double regulation etc. of certification authorities.

Subsection (2):

Subsection (2) authorises the National Telecom Agency to issue orders to a certification authority to ensure compliance with the provisions of the Act.

Point 1) authorises the National Telecom Agency to order a certification authority to notify the Agency, see section 16, and order it to submit further information if a notification is inadequate.

Under point 2), the National Telecom Agency may order a certification authority to submit reports to the Agency, see section 17, including orders to submit further information if a report is inadequate.

Under point 3), in cases where the Agency finds that a certification authority does not comply with the provisions of the Act, the National Telecom Agency may order a certification authority to bring the matter in question concerning the certification authority's activities into conformity with the Act.

In case of concrete suspicion about a criminal offence, the provision cannot be applied to order the relevant certification authority or system auditor to submit further information or to investigate matters related to the suspicion. In such case, the authorities must apply the rules of criminal law. This also applies to the obligation to submit information in section 19, subsections (1) and (2), and section 20, subsections (2) and (3), and to the performance of an extraordinary system audit, see section 18 (5).

Subsection (3):

In connection with orders issued in pursuance of subsection (2), the National Telecom Agency must stipulate a time limit for the certification authority's compliance with the order. The length of the time allowed will depend on the concrete situation, including whether the National Telecom Agency finds that it might be necessary to use its powers under subsection (6) to deprive a certification authority of the right to issue qualified certificates.

Subsection (4):

The National Telecom Agency is authorised under subsection (4) to impose daily penalties on a certification authority which does not comply with orders issued in pursuance of subsection (2).

Subsection (5):

In pursuance of subsection (5), the National Telecom Agency may carry out an extraordinary system audit at a certification authority issueing qualified certificates. The

provision enables the National Telecom Agency to give itself and the management of the certification authority an overview of a number of matters in the company on which clarification is sought by the National Telecom Agency in view of the existing information. The National Telecom Agency will appoint a system auditor to carry out the extraordinary system audit and specify the detailed framework for carrying it out. The appointed system auditor may either be the auditor appointed by the certification authority or another auditor.

The National Telecom Agency may order the certification authority to pay the cost of the extraordinary system audit. This would normally be the case if the reason for the extraordinary system audit was submission of insufficient information to the National Telecom Agency by the management of the certification authority or the appointed system auditor.

Subsection (6):

In pursuance of subsection (6), the National Telecom Agency may deprive a certification authority of its right to use the designation qualified certificates in gross cases where the certification authority, despite orders and the imposition of daily penalties, has failed to comply with the Agency's orders and has grossly and repeatedly violated the provisions of the Act, or if the certification authority suspends its payments or goes into liquidation.

It is a prerequisite for applying the authority vis-à-vis a certification authority that the situation calls for direct protection of the users of the issued certificates.

Subsections (7) and (8):

The provisions states that a decision of the National Telecom Agency under subsection (6) to deprive a certification authority of its right to use the designation qualified certificates may be brought before the courts. At the same time, rules are laid down on situations in which a decision to bring a decision of the National Telecom Agency before the courts can have suspensive effect.

Section 19:

The provision enables the National Telecom Agency to require data to be submitted with a view to undertaking its supervisory task.

As mentioned above in the notes on section 18 (2), the obligation to submit information cannot be used to order a person or a company to submit further information in cases of concrete suspicion about a criminal offence.

Subsection (1):

The provision gives the National Telecom Agency the right to collect information from all certification authorities that issue qualified certificates, and from other companies and persons, to enable the Agency to assess whether they are covered by the Act.

Subsection (2):

Subsection (2) requires the management and system auditor of a certification authority to inform the National Telecom Agency immediately on matters of vital importance to the certification authority's continued operation. Major system breakdowns at a certification authority or problems in complying with the requirement in section 5 (1), point 5),

concerning the financial resources of the certification authority, including cases where the authority goes into liquidation or suspends its payments, are examples of situations in which the National Telecom Agency should be informed. The National Telecom Agency's real possibility of taking action against a certification authority that for one reason or another had difficulty in complying with the Act will depend largely on the Agency receiving the relevant information in time.

Section 20:

Subsection (1):

The National Telecom Agency is empowered to order a certification authority to appoint a new system auditor within a stipulated time if its system auditor is found clearly unsuitable for his task.

The auditing by the system auditors of the activities of a certification authority forms an important part of the regulation of the certification authorities, and it is thus vitally important that the system auditor's audit is of a high quality. The National Telecom Agency is therefore only empowered to intervene in cases where an auditor of a certification authority is found clearly unsuitable for his task.

Subsection (2):

Subsection (2) empowers the National Telecom Agency in special cases to order a system auditor of a certification authority to provide information concerning the certification authority without the consent of the management of the certification authority. The purpose of this is to give the National Telecom Agency a possibility of assessing whether there are problems with the activities of the certification authority in relation to the provisions of the Act.

Subsection (3):

Under subsection (3), the certification authority and the system auditor must each submit a report to the National Telecom Agency in the event of a system auditor relinquishing his task. The National Telecom Agency will thus become aware of any problems within the certification authority.

As to the application of the provisions in subsections (2) and (3), in cases of concrete suspicion about a criminal offence, reference is made to the notes above on section 18 (2).

Section 21:

The provision states that decisions made by the National Telecom Agency under this Act, or provisions laid down in pursuance thereof, cannot be referred to other administrative authorities. Complaints concerning decisions by the National Telecom Agency thus have to be referred to the courts or the Ombudsman.

The decisions made by the National Telecom Agency in pursuance of the Act must be expected mainly to concern operational and technical matters relating to the activities performed by a certification authority.

The number of certification authorities to be covered by the Act in the near future must be expected to be modest. Since a board of appeal must have thorough technical knowledge of electronic signatures and of the activities of a certification authority to be able to assess

decisions made by the National Telecom Agency and will probably only have to make decisions in a small number of cases, it has not been found relevant to spend resources on such a board.

Section 22:

The Minister of Research and Information Technology is authorised to lay down rules to the effect that the costs incurred by the State in connection with the National Telecom Agency's regulation be paid by the certification authorities that issue qualified certificates.

It is intended to distribute the costs between the contributing certification authorities on the basis of calculations of the resources spent by the National Telecom Agency on its regulation of the individual certification authorities.

Subsection (2) provides authority to recover outstanding contributions by means of distraint.

Part 10. International issues ➦

Section 23:

The provision implements Article 7 of the Directive and lays down the conditions to be met by certificates issued by certification authorities established in a third country - i.e. a country outside EEA - in order for them to be recognised as legally equivalent to certificates issued by a certification authority established within the EEA.

It follows from section 11 that a certification authority established in Denmark that guarantees qualified certificates issued by a certification authority from a third country will be liable for such certificates as regards the types of losses covered by the provision in the same way as the Danish certification authority guarantees certificates issued by itself.

Part 11. Criminal liability ➦

Section 24:

The provision sets out the provisions that will give rise to penalties if violated.

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

Part 12. Coming into force etc. ➦

Sections 25-26:

The Act will come into force on 1 October 2000.

This allows for more detailed rules to be drawn up implementing the authority given in this Act to the Minister of Research and Information Technology and the National Telecom Agency.