Electronic signatures in Denmark: free for all citizens

JAN HVARRE

Both the Directive and the Danish Act establish general principles for the approval of electronic signatures

Historical background

■ Early Danish start

In the late eighties and the early nineties, the general view in Denmark was that the establishment of a public key infrastructure (PKI) was an important condition for the popularisation of electronic signatures.

In 1996, the first draft for a Danish law on electronic signatures was prepared, to be followed by a revised version in 1998. The ambition of the draft bill was not only to lay down requirements for electronic signatures and certificate issuing key centres ("Certification Authority"), but also to govern how electronic signatures meet requirements in Danish law where an agreement or exchange of messages must be in writing and signed. Thus, the idea was that such requirements could be fulfilled by the exchange of electronic messages applied with an electronic signature.

The implementation of the draft bill implied a review of the requirements as to formality in the entire Danish legislation, which was assumed to include more than 10,000 rules and regulations with formal requirements for a written signature, which would be influenced by the legislation. It was discussed whether to pass a decision on every single rule and regulation where an electronic signature was to be accepted ("opt in" model), or generally to consider electronic signatures as fulfilling the formal requirements of the rules and regulations unless otherwise decided concerning the rule in question ("opt out" model).

The review was, however, somewhat time-consuming and thus the draft bill was overtaken by the Directive from the European Parliament on electronic signatures and was therefore never implemented.

■ The EU Directive on electronic signatures

On 13 December 1999, the EU issued Directive no 99/93 on a Community framework for electronic signatures.[1] A EU Directive does not impose direct obligations on the citizens in a member state. The member states are, however, obliged to implement the regulation of the Directive into national law within a given time limit. Dependent on the form of the Directive, member states are left with more or less free hands as to the actual drafting of the national legislation.

According to the European Commission, all countries have implemented the Directive, and thus it may be expected that all member states have rules on electronic signatures generally corresponding to the Danish regulation. In Denmark, the Directive has been implemented by means of Lov om elektroniske signaturer, the Danish Act on Electronic Signatures, nr. 417 of 31 May 2000 ("The Danish Act").

Both the Directive and the Danish Act establish general principles for the approval of electronic signatures. Certain advanced signatures based on qualified certificates are granted special advantages. The Directive and the Danish Act concentrate on the role of the centres issuing electronic keys ("Key Centres"). Moreover, article 5 of the Directive establishes general requirements that advanced electronic signatures based on a qualified certificate and created by a secure signature creation device shall be deemed to:

- comply with the legal requirements of a signature in relation to data in electronic form to the same extent that a handwritten signature meets these requirements in relation to data in paper form, and
- be admissible evidence in legal actions.

Moreover, article 5 (2) also provides that member states must ensure that advanced electronic signatures are not deemed legally invalid and inadmissible evidence in legal actions only because they

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).

- are electronic;
- are not based on a qualified certificate;
- are not based on a qualified certificate issued by an accredited key centre; or
- are not created by a secure signature creation device.

Finally, the Directive prohibits, as part of the general efforts to secure free movement of goods and services between member states, that a country requires that the Key Centres must obtain prior certification.

Danish law on electronic signatures

■ Scope and definitions

Efforts have been made to keep both the Directive and the Danish Act technology neutral. This appears from the definition of an electronic signature in the Danish Act, section 3(1):

Data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et signaturgenereringssystem, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret.	Electronic data attached to other electronic data by a signature creation device and which are used for verifying that these originated from the person indicated as signatory, and that they have not been amended.

Thus, it is required that a "device" is used for creating the electronic signature. Stating your name at the end of an e-mail will not meet this requirement. It is, however, in principle not necessary to involve a Key Centre to meet the requirements of the definition. However, most of the provisions in the Danish Act provide for procedures that indicate the use of a key centre in a Public Key Infrastructure (PKI) is presumed to be the most common procedure.

A further requirement is that a natural person must always issue the electronic signature. An electronic signature issued by a machine will therefore not qualify as an electronic signature under the Danish Act.

■ Variation of electronic signatures

In principle, all electronic signatures are subject to the Danish Act. However, a distinction is made between different types of signatures with different effects, depending on whether the signature is regarded (1) "advanced", (2) is issued based on a "qualified" certificate and (3) is created by a secure signature creation device.

■ Advanced electronic signatures

An advanced electronic signature is a signature fulfilling the following four requirements, see the Danish Act, section 3(2):

- It must be uniquely linked to the signatory.
- It makes it possible to identify the signatory.
- It is created using means under the exclusive control of the signatory.
- It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Requirements 1, 2 and 4 would be met by the use of an ordinary electronic signature based on the use of the signatory's secret key using complete encryption or creation of a hash value of the signed message. Requirement 3 can be met by means of prior agreement between the signatory and the receiver, or by involving a trustworthy third party.

■ Qualified certificates

In order to provide the possibility of issuing especially trustworthy certificates, both the Directive and the Danish Act contain the concept of a "qualified certificate". This is a protected designation, as only certificates meeting the requirements mentioned below can be designated "qualified certificates".

To classify as a qualified certificate, the certificate must be signed with the Certification Authorities advanced electronic signature, see section 4(3) of the Danish Act. Moreover, according to section 4(2) the certificate must meet the following requirements as to the level of information:

- The certificate must identify the "item" being qualified, and state the name and registered address of the Certification Authority, the signatory's name or pseudonym (in such event specifying that it is a pseudonym) and any further information regarding the signatory, including information providing an unambiguous identification of the signatory.
- The qualified certificate must contain information regarding the validity period of the certificate and any limitations as to object and amount, which define the application of the certificate.
- The qualified certificate must contain an identification code and the signature verification data corresponding to the signature creation data, which are controlled by the signatory at the time of the issue.

At present, only a very limited number of Danish acts provide for the use of an electronic signature

■ Secure Signature Creation Devices

Further, a distinction is made between ordinary signature creation devices and "secure" signature creation devices. According to the Danish Act section 14-15, a signature creation device must meet certain requirements to obtain the designation "secure". In this connection, the Danish Act introduces a system according to which the Danish Ministry of Science, Technology and Innovation appoints a test centre, which is responsible for controlling whether the signature creation device meets the requirements. The Ministry has not yet appointed such centre, probably because no test centre has found it commercially feasible to undertake this task. Danish parties looking for verification that their signature creation device is "secure" therefore must contact a test centre in another member state within EU, cf. section 15(3) of the Danish Act.

■ Legal effect of electronic signatures

The Danish Act anticipates a situation where the individual Danish acts generally accept electronic messages signed electronically. Section 13 of the Danish Act states that any requirement in the legislation of signature on electronic messages shall be deemed fulfilled if the message is:

- provided with an advanced electronic signature;
- based on a qualified certificate; and
- created by a secure signature creation device.

This means that any person or business acquiring an electronic signature fulfilling the requirements set out in the Danish Act on Electronic Signatures can be confident of fulfilling any future legislative requirements. At present, only a very limited number of Danish acts provide for the use of an electronic signature.

■ Requirement for the business of the Certification Authority: the identification requirement

A Certification Authority operating in Denmark does not need to be authorized, as this would be contrary to the EU Directive. The Certification Authorities must, however, fulfil a number of requirements, especially if they want to issue qualified certificates. Some of these requirements are laid down in a departmental order issued by the Danish Ministry of Science, Technology and Innovation ("the Departmental Order")[2].

First of all, the Certification Authority is required to have a written certification policy and a certification practice, both of which shall be made available to the public, cf. section 2 of the Departmental Order. Moreover, the CA must take out an insurance covering damage arising out of its business operations, cf. section 5 of the Departmental Order.

Secondly in connection with the issue of qualified certificates, the Certification Authority must verify the identity of the person or business by requiring physical appearance at the office of the Certification Authority, (section 6 of the Departmental Order), or at the office of a representative appointed by the Certification Authority, (section 8 of the Departmental Order). This requirement can only be deviated from if the Certification Authority already knows the signatory.

The requirement of physical appearance is relatively far-reaching, especially when considering the fact that the Certification Authority is already motivated to perform a thorough check because of the "presumption of negligence", for which see further below. The requirement is not contained in the Directive, which only requires the use of "appropriate means in accordance with national law".[3]

The Certification Authority may appoint other businesses or authorities to be local registration units performing the identity check on its behalf. Thus, a number of Danish Certification Authorities have chosen to issue qualified certificates using either local post offices or banks as local registration units in order to make is as easy as possible for the citizens to appear in person.

[2] Bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til nøglecentre.
[3] Recital 21.

■ Liability: reversed burden of proof

Section 11 of the Danish Act lays down a strict liability for Danish Certification Authorities issuing qualified certificates:

Nøglecentre, der udsteder kvalificerede certifikater til offentligheden, eller som over for offentligheden indestår for sådanne certifikater udstedt af et andet nøglecenter, er ansvarlig for tab hos den, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes,

- at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet,
- at certifikatet ikke indeholder alle oplysninger som krævet i henhold til § 4,
- manglende spærring af certifikatet, jf. § 9, stk. 2,
- manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. § 9,

stk. 1 og 3, eller tilsidesættelse af § 7.
Stk. 2. Et nøglecenter pådrager sig erstatningsansvar efter stk. 1, medmindre nøglecentret kan godtgøre, at nøglecentret ikke har handlet uagtsomt eller forsætligt.
Stk. 3. Et nøglecenter er ikke ansvarlig for tab opstået som følge af anvendelse af et kvalificeret certifikat uden for de formålsbegrænsninger, som gælder for certifikatet, eller for
tab opstået som følge af en overskridelse af de beløbsbegrænsninger, som gælder for certifikatet,

- forudsat at de pågældende begrænsninger tydeligt fremgår af certifikatet, jf. § 4, og på forespørgsel oplyses, jf. 9, stk. 1 og 3.

Stk. 4. Stk. 1-3 kan ikke ved forudgående aftale fraviges til skade for skadelidte.
Stk. 5. Stk. 1-3 finder ikke anvendelse, i det omfang tabet dækkes efter lov om visse betalingsmidler.

The key centres, which issue qualified certificates to the public, or which towards the public vouch for such certificates issued by another key centre, is liable for any loss incurred by those who reasonably rely on the certificate if the loss is due to:

- the information stated in the certificate not being true at the time of the issue of the certificate;
- the certificate not containing all information required under section 4;
- lack of blocking of the certificate, see section 9(2);
- lack of or misinformation regarding blocking of the certificate, expiry date of the certificate, or if the certificate contains any limitations as to objects or amounts, see section 9(1) and (3); or
- non-observance of section 7.

(2) A key center incurs liability pursuant to sub-section 1 unless the key center can prove that the key center has not acted negligently or willfully.
(3) A key center is not liable for

- Loss occurred in relation to the use of a qualified certificate beyond the limitations as to objects applicable to the certificate; or for
- loss occurred due to an excess of the amount limitations applicable to the certificate;
- provided that the said limitations are explicitly stated in the certificate, see section 4, and are notified upon inquiry thereof, see section 9(1) and (3).

(4) Sub-section 1-3 cannot be derogated from to the detriment of the claimant by prior agreement between the parties.
(5) Sub-section 1-3 are not applicable if the loss is covered according to the Danish Act on certain means of payment (lov om visse betalingsmidler).

As it appears, the Certification Authority is liable for damage caused to any person or business, which reasonably relies on the certificate unless the Certification Authority can prove that it has not acted negligently. In other words, the Certification Authority is subject to a so-called presumption of negligence.

The Certification Authority is not, however, liable for damages for loss arising out of the use of a qualified certificate beyond the limitations as to the object and amount that applies to the certificate. Naturally, this implies that the limitations in question are clearly stated in the certificate. The liability of the Certification Authority cannot be derogated from to the detriment of the claimant by prior agreement between the parties.

The OCES signature is approved by the Danish Data Protection Agency for use by public authorities when exchanging sensitive information with citizens

The public sector as the driving force

The public sector in Denmark has found it natural and necessary that the use of electronic signatures should be encouraged on the initiative of the public authorities. The widespread use of electronic signatures requires a certain volume, and also a standardization that ensures that the applied devices using PKI are compatible. In this connection, it is important to bear in mind that the public sector itself may save large sums if electronic signatures are commonly used. This is because of the massive exchange of information between citizens and public authorities and between public authorities.

Therefore, the Danish government has launched a project called OCES ("Offentlige Certifikater for Elektroniske Services", or "Public Certificates for Electronic Services"). The purpose of the project is to facilitate the take-up of electronic signatures and thereby the development of electronic public administration. The project implies the creation of a standard PKI in which the source code for the signature creation device is made public. The project also implies that all Danish citizens may obtain a free electronic signature.[4]

Based on a EU supply procedure[5], the Danish Ministry of Science, Technology and Innovation has appointed TDC A/S, the largest telecommunication company in Denmark, to perform the issuing of electronic signatures. The OCES certificate standard covers three types of certificate:

- The personal certificate, verifying a person's identity.
- The employee certificate, verifying the identity of a person and his or her status as an employee of a certain business.
- The business certificate, verifying that the holder of the certificate is in fact representing the business stated in the certificate.

So far, the OCES certificate is only based on software. Notwithstanding that the solution basically intends to ensure the use of the certificate between citizens and public authorities and among public authorities, it can also be used in the private sector. So far, however, primarily public authorities offer to accept documents signed electronically by use of the OCES signature, including schools, colleges and universities, the tax authorities and a number of local authorities, for instance

All Danish citizens may order a free electronic signature by contacting TDC A/S via the internet. In order for the signature to be issued, the citizen in question must state his or her civil registration number and e-mail address. TDC A/S then forwards a unique HTML address to be used for downloading the electronic signature by e-mail. However, the PIN code necessary for downloading the electronic signature is sent by ordinary mail to the physical address listed with the residence register of the person in question. Apart from situations where unauthorized persons order an electronic signature using another person's civil registration number, and also have access to, or is willing to force access to, the private ordinary mail of the person in question, the system is thus relatively secure.

The OCES signature is approved by the Danish Data Protection Agency for use by public authorities when exchanging sensitive information with citizens. However, the system does not fulfil the requirement of personal appearance, on which the issue of qualified certificates is based (see discussion above). Therefore, it appears somewhat peculiar that the Danish Ministry of Science, Technology and Innovation has chosen an identification procedure which results in the issued certificates not meeting the requirements set out in section 13 of the Danish Act on Electronic Signatures. Otherwise, the OCES signature would meet the requirements for electronic signatures following any future legislation in the area. However, the Ministry has probably decided to attach the ease of obtaining an electronic signature with greater value in order to facilitate the highest possible take-up of the electronic signature.

The free electronic signature was made available in March 2003. However, the distribution of the electronic signature has not been a success so far. Shortly after the introduction, it was possible to complete one's tax return by the use of electronic signature. However, only 7,000 of Denmark's 3.9 million taxpayers did so. At the time of writing this article, only 145,000 Danish citizens, less than three per cent of Denmark's population, holds the free OCES signature. The reason for the low take-up is partly that many public institutions, including the taxation authorities, still offer entry of and access to information via the internet using a PIN code only, partly that less than 25 per cent of the citizens actually know that the OCES signature is free[6]. As TDC will receive a bonus if it distributes the OCES signature to at least 350,000 citizens by June 2004, TDC has launched a marketing campaign, by which citizens that register for the OCES signature can participate in a competition with a trip to Disney World in Florida is the main prize. TDC also finds support in the fact that the numbers of public services available through the OCES signature is rapidly growing. Notwithstanding this development, it is considered unlikely that TDC will issue 350,000 digital signatures in time.

In contrast, the Danish banks have issued more than a quarter of a million electronic signatures in connection with home banking, without issuing any trips to Disney World in the process. ■

[4] Read more at (Danish sites) http://www.videnskabsministeriet.dk/cgi-bin/theme-list.cgi?theme_id=7471, http://privat.tdc.dk/digital and https://www.signatursekretariatet.dk/frontpage.html.
[5] Project competition with limited participation under Directive 92/50/EEC as modified by Directive 97/52/EC, art. 13.
[6] http://politiken.dk/VisArtikel.iasp?PageID =301322&TemplateID=552.

Jan Hvarre is attorney-at-law at the IT-law department of the law firm Kromann Reumert, Denmark. Has worked with IT-law and Intellectual Property Rights since 1998. He teaches IT law on the MA programmes at the Aarhus School of Business as well as at the assistant attorney course, an obligatory course for law graduates wishing to become attorneys.

jhv@kromannreumert.com
www. kromannreumert.com