Digital Certificates and Certification Services

Rolf Riisnæs

1 Introduction ………………………………………………………………... 132

2 Market, Technology and Infrastructures ……………………………….…….. 132

2.1 Electronic Communication – Challenges and Terminology ……………... 132
2.2 Public Key Encryption and Electronic Signatures ………………………. 134
2.3 Digital Certificates …………………………………………………….…. 136
2.4 Certification Services ……………………………………………….…. 138
2.5 Certificate Valdation ……………………………………………………... 139

3 Regulating Certification Services - the Electronic Signature Act ………… 140

3.1 Implementing Directive 1999/93/EC …………………………………….. 140
3.2 Scope and Area of Application …………………………………………... 141
3.3 Definitions ………………………………………………………………... 142
3.4 CSPs Providing Qualified Certificates …………………………………… 144
3.5 Data Protection …………………………………………………………… 147
3.6 Legal Recognition of Certificates Issued by a CSP Established Outside Norway ……………………………………………………………………… 148
3.7 Legal Recognition of Electronic Signatures ……………………………... 148

4 Other Legal Framework Facilitating Electronic Communication and Certification Services ………………………………………………………… 149

4.1 Law reforms - 'eRegelprosjektet' etc 149
4.2 Public Sector Regulations ………………………………………………... 150

1 Introduction

It is now widely recognised that public key encryption, digital certificates and certification services may be an important requisite for electronic communication in open networks. Certificate technology and certification services may support electronic signatures, but they are neither the only technology available for this purpose, nor do electronic signatures utilize the entire potential of certificate technology.

The aim of this article, is to take a closer look at the characteristics of digital certificates and certification services, and the legal framework that relates to such certificates and services.

After some introductory remarks, there is a brief description of public key encryption and electronic signatures, followed by a discussion about digital certificates and the management of such certificates. The rest of this article deals with the legal framework of electronic communication and certification services, including a presentation of the Electronic Signature Act.[1] The Act implements the Directive 1999/93/EC[2] on a Community framework for electronic signatures into Norwegian law. Similar Acts exist in the other Scandinavian countries. Finally, one will find an introduction to other law reforms undertaken to facilitate electronic communication and certification services in Norway.

2 Market, Technology and Infrastructures

2.1 Electronic Communication – Challenges and Terminology

Electronic communication is growing, not least in open networks such as the Internet, recognised by the fact that the parties can enter into commercial or administrative relations without any prior agreement between them. Undertaking such operations in open networks is subject to numerous challenges.[3]

Firstly, there is a lack of transparency in such networks. Any party could operate under any identity or claim any authority on the Internet, and it is generally difficult to establish whether or not the facts claimed represent the truth.

Secondly, there is a lack of durability in the electronic medium. An electronic message may also be changed without leaving any trace. The combination of these two characteristics may cause evidential problems if a dispute arises.

Thirdly, there is still a lack of tradition and experience in electronic commerce. Traditionally, in commercial relations, one used to have a "gut feeling" with regard to the circumstances under which one could expect a

[1] *See* Act on Electronic Signature of 15th June 2001, No 81 (hereinafter also referred to as 'the Act'), available (in Norwegian) from "http://www.lovdata.no/all/hl-20010615-081.html".

[2] Hereinafter also referred to as 'the Directive'.

[3] *See, e.g.,* Communication from the EC Commission, "Ensuring security and trust in electronic communication – towards a European framework for digital signatures and encryption", Brussels, 8th October 1997, COM(97)503; Schneier, Bruce, *Secrets and Lies – Digital Security in a Networked World,* Wiley, New York 2000.

transaction to work. In electronic commerce, one often does not have this feeling. This may result in a lack of trust in electronic commerce as a secure and effective way of doing business.

Fourthly, the computerisation and automated systems require control mechanisms to be formalised. A computer does not (yet) have the ability of a human being to evaluate the available facts of the situation and decide whether it should be considered acceptable or not. The reliability of human intuition with regard to trustworthiness in such relations might be questioned, but in practice we rely heavily on it in day-to-day business practice.

Fifthly, data distributed through the network is potentially being disclosed to someone other than the intended users.

Finally, it may be necessary to comply with one or more legal requirements. Such requirements may be related to *eg* authentication, evidence or requirements as to form.

To a large extent, however, the challenges are related to the issue of evidence and the matter of trust. The question is: what do the parties need to obtain the level of trust necessary for them to dare completing the transaction? In practice, this should not be expected to be an entirely rational decision based on a careful evaluation of the risks involved and the measures taken. In many cases, it is probably based on common sense and a broad evaluation of the circumstances. Commerce is about managing risks. What is sought is not a "bullet-proof" solution but adequate security at a reasonable cost; the result of a process referred to by Schneier as the "security trade-off".[4]

Some basic terminology related to the security requirements should be explained at the outset. First of all, one might want to be able to verify the claimed identity of the party with which/whom one communicates. This functionality is commonly described in terms of "authentication". One might also like to ensure that messages are not changed, accidentally or on purpose, during transmission. This concern relates to "data integrity". Further, one might want to collect proof that a given message was actually sent by a given party – a functionality referred to as "non-repudiation".[5] Finally, one might want to ensure that a message is withheld from any parties that are not authorised to read the message. This concern is about "confidentiality".

However, as indicated above, such requirements should be related to the potential risk of the transaction in question. For certain operations, a high level of security is required, *eg* if health information is to be transmitted through open networks. For other transactions one may be satisfied by establishing a reasonable certainty about the other party's identity or powers. This should be reflected in the interpretation of the terms describing the relevant security

[4] *See* Schneier, Bruce, *Beyond Fear – Thinking Sensibly About Security in an Uncertain World*, Copernicus Books, New York 2003, ISBN 0-387-02620-7.

[5] This is probably not an accurate use of the term, but it seems it has come to stay. The term was used by cryptographers to express that if one's digital signature algorithm is not breakable, no third party could forge one's signature, thus providing proof that a certain private key was used to sign the message. This does not necessarily provide proof regarding the identity of the sender and, concomitantly, it does not necessarily prevent, in law, the person to whom the private key is formally ascribed, from repudiating the assumption that he/she is the sender of the message in question.

services. In this sense Clarke explains that ”Authentication refers to a process whereby a degree of confidence is established in an assertion. The assertion might relate to identity, but in many cases it does not.”[6] These dynamics should be reflected by the certificate technology. A digital certificate, as discussed in more detail below, might be one of the measures available to the process of establishing confidence in an assertion about an identity or other data.

The term “identity” is usually related to a natural person and commonly associated with the name of that person. It has been discussed whether this is an appropriate way to use the term with regard to certificates, the purpose of which are to distinguish a legal or natural person or electronic agent from other entities.[7] The discussion arises partly because there is no common understanding of any globally unique identifier.[8] Furthermore, one might distinguish between “identity”, “identifier” and/or “identification data”. This discussion will not be entered into here. For present purposes the notions of “identity”, “identifier” and “identification data” are used simply to denote data intended to distinguish one entity from other entities.[9] Whether or not such distinctions can be made in a certain transaction depends partly on which data the user already has. For instance, a name and date of birth might be sufficient to distinguish one person from another within a certain user community. However, if the verifier does not know the person’s date of birth beforehand, this piece of information will not help him to identify the person.

Public key encryption, digital certificates and certification services, may support electronic communication to overcome the aforementioned challenges.

2.2 Public Key Encryption and Electronic Signatures

Digital certificates are commonly associated with public key encryption. Public key encryption is encryption based on the use of two different but related keys – one key for encryption and another key for decryption – where it is not possible to compute one key from the other. One key is kept secret to the key-holder (the private key). The other key of the key-pair may be communicated to others (the public key). Digital data encrypted with the public key can only be decrypted with the corresponding private key and the encrypted data are thus kept confidential and will only be accessible to the holder of the private key.

To obtain electronic signatures, the use of the keys is reversed. What is encrypted with the private key can only be decrypted with the public key. Thus, if a message can be decrypted with a person’s public key one can be pretty sure

[6] Clarke, Roger, *Why Do We Need PKI? Authentication Re-visited*, Review Draft of 28 January 2002, Introduction, “http://www.anu.edu.au/people/Roger.Clarke/EC/PKIRW02.html”.

[7] *See, e.g.,* Clarke, Roger, *The Re-Invention of Public Key Infrastructure*, December 2001, available from “http://www.anu.edu.au/people/Roger.Clarke/EC/PKIReinv.html”.

[8] *See, e.g.,* Ellison, Carl M., *Improvements on Conventional PKI Wisdom*, 1st Annual PKI Research Workshop – Proceedings, (2002) p. 165-175. *See* also Ellison, Carl and Schneier, Bruce, *Ten Risks of PKI: What you’re not being told about Public Key Infrastructure*, Computer Security Journal, vol XVI, no 1, 2000, available from “http://www.counterpane.com/pki-risks.html”.

[9] By “entity” is meant a legal or natural person or an electronic agent.

that it has been encrypted with the corresponding private key. The encrypted message becomes the "signature" of the sender. The signature is a function of the message and so it is also unique to the message.

In real life, the situation is a bit more complicated. What is being signed is actually a one-way hash (ie, mathematical abbreviation or "digital fingerprint") of the message. The result of this operation is appended to the message and this is what is called the "signature".[10] An electronic signature based on the use of public key encryption is frequently referred to as a "digital signature".[11]

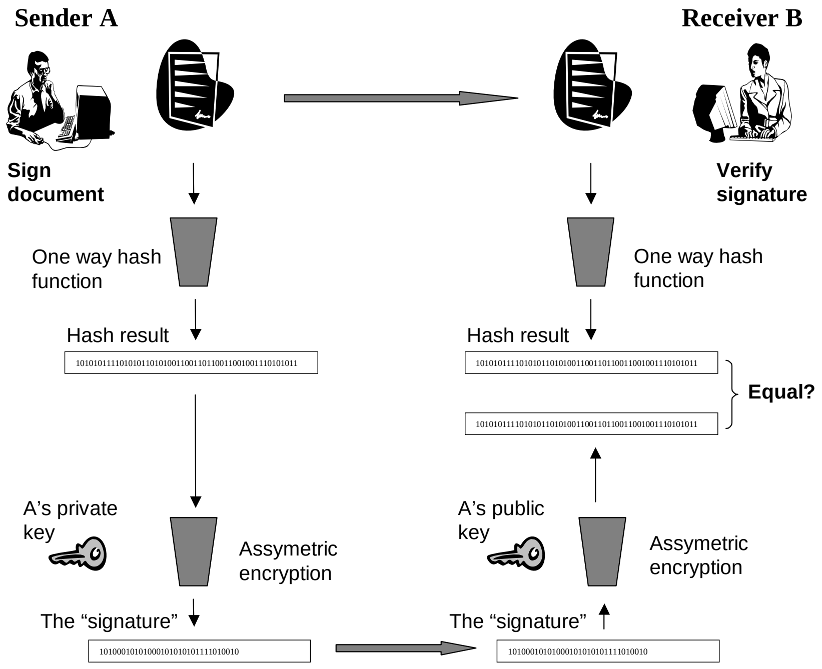


Figure 1: The digital signature process

Also in real life, no one really encrypts a message with a public key (largely because of the relatively lengthy time that such a process usually takes). Operational systems use a hybrid approach combining symmetric and public key encryption. A standard encryption algorithm is used to encrypt the message with a random key (called a *session key*). That key is encrypted with the public key.

[10] The use of the term "signature" for this purpose is opposed by several commentators. I agree with this criticism. However, use of the term in this context seems to have come to stay. Therefore, focus should now be put on the possibilities and limitations found in the functionality of the technology.

[11] *See* more about electronic signatures in *e.g.* Magnusson Sjöberg, Cecilia, *Managing electronic signatures*, in Ruth Nielsen et.al. (eds.), EU Electronic Commerce Law, DJØF Publishing 2004, p. 95-108.

As intimated above, the reason for this process is speed.[12] The receiver first decrypts the session key with his private key. Then the message can be decrypted with the session key.

2.3 Digital Certificates

Given the potential of public key technology, among other questions, one may ask: "How do I know who holds the key?" One way or another, the key will have to be associated with some other data. The common approach is that the public key is included in an electronic record called a "certificate", together with some other pieces of information, and signed with the digital signature of the provider of the certificate.

Broadly speaking, a *certificate* is an electronic record that, by its content, associates certain data with a natural or legal person or an electronic agent. The certificates can be divided into (at least) two categories: (i) certificates that associate a public key with an identifier of a legal or natural person or electronic agent; (ii) certificates that associate an entity or a public key with an attribute or role – *eg*, an authorisation to act on behalf of a legal person or to order payments from a bank account. The first category may be called "ID certificates" or "public key certificates", and the second category "role-based certificates" or "attribute certificates". In the Electronic Signature Directive, the term "certificate" is defined as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person" (see Article 2(9)). Following current technical standards, only a physical person can be the holder of a *qualified certificate*, whereas even other entities can hold other certificates.[13] There are international standardisation work addressing the profiles of attribute certificates. This is on the agenda of, amongst others, IETF[14] and ETSI[15].

The two types of certificates may have the same structure and main characteristics but there are some major differences. Firstly, the attribute

[12] Encryption of the message by the session key, followed by encryption of the session key by the public key, will usually be much quicker than encryption of the entire message by the public key.

[13] ETSI TS 101 456 *Policy requirements for certification authorities issuing qualified certificates* is limited to natural persons, while ETSI TS 102 042 *Policy requirements for certification authorities issuing public key certificates* supports certificates even for automated systems. Both policies are available from "http://portal.etsi.org/esi/el-sign.asp".

[14] The Internet Engineering Task force (IETF) has published a proposed standard protocol RFC 3281 "An Internet Attribute Certificate Profile for Authorization" (April 2002), available from "http://www.ietf.org/rfc/rfc3281.txt".

[15] *See* ETSI TS 102 158 *Policy requirements for CSPs issuing attribute certificates* (October 2003). Work by ETSI in the area is done in close co-operation with CEN/ISSS within the European Electronic Signature Standardisation Initiative (EESSI) work programme.

certificate does not necessarily contain a public key.[16] Secondly, the processes of issuing the certificates are different. Given that a person or agent has a trustworthy ID certificate, an attribute certificate can be issued and distributed over the network without any further authentication between the parties. Thirdly, the issuer of the attribute certificate will usually be different from the issuer of the ID certificate. Once a person has an ID certificate, his employer may for instance issue an attribute certificate attesting the relationship with the employee. Fourthly, attribute information usually does not have the same lifetime as an ID certificate. And finally, although ID certificates can be *pseudonymous*,[17] the attribute certificates could be *anonymous* by simply attesting that the holder of a certain key is authorised to perform certain actions without revealing the person's identity. However, the more common approach seems to be to associate the attributes with an identifier or an unambiguous link to a public key certificate.[18]

The two types of certificates may be used separately or in combination. However, the use of attribute certificates may be more flexible when built on top of existing ID certificates. This flexibility is due to the fact that once a person or agent has the capability of identifying him-/her-/itself over the network by using a certain key (pair), attributes can be attached to the same subject by different entities. An employer will be an authority with regard to issuing attribute certificates to his employees. A bank will be an authority with regard to issuing attribute certificates related to banking services. And a principal will be an authority with regard to issuing an attribute certificate to his agent. In principle, these attribute certificates could be validated using the same pair of keys, which is attested by an ID certificate. This allows the holder to use only one (or, for security reasons, a few) pair(s) of keys, and prove his different roles by way of

[16] According to Brands, an attribute certificate that does not contain a public key, is not really a certificate, *see* Brands, Stefan A., *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy,* The MIT Press 2000, p. 12. Although the term certificate may for practical reasons be limited to signed assertions about a public key, the common approach is to include even other forms of credentials.

[17] *See* Directive 1999/93/EC on a Community framework for electronic signatures, Article 8(3) ("… Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name"), and Annex I para c) ("Qualified certificates must contain: … c) the name of the signatory or a pseudonym, which shall be identified as such").

[18] Attribute certificates issued pursuant to ETSI TS 102 158 *Policy requirements for CSPs issuing attribute certificates,* shall contain an unambigous link to a Qualified Certificate, *see* Annex A para d). According to the RFC 3281 specification, the attribute certificate links the attributes to an identity, whereby validation of the attribute certificate may require the validation of a chain of public key certificates. The attribute certificate might contain a unique reference to the public key certificate on which it is based. Alternatively, the attribute certificate may contain an identifier of the certificate holder. This might give the signer freedom to choose which ID certificate (if he has more than one) should be used to validate the attribute certificate, *e.g.,* by different communities. However, this method faces the problem of matching the identification data of the two certificates. Taking into consideration that the certificates will be issued by different entities, matching the identifiers may not be a trivial task. Should anonymous attribute certificates be required, the RFC 3281 (7.3) allows the "holder" field to contain, *e.g.,* the hash of a public key, in effect confirming the authorisation of the attribute to the holder of the key pair.

the attribute certificate relevant to the transaction in question. Different user communities might develop community-specific attribute profiles.

Yet we also have to make another distinction between different types of certificates. This relates to a relatively lengthy discussion about “key-usage”. For security purposes, it is recommended not to use the same pair of keys for operations such as encryption, authentication and digitally “signing” electronic records. We will not go here into a detailed explanation of this. The recommendation for different key pairs is reflected in standards for certificate policies and profiles. There is a field in the certificate called “key-usage” dedicated to distinguishing between the different uses. Key-usage should be set to “encryption” if the public key is to be used for encryption purposes. It should be set to “non-repudiation” when the related key-pair is intended for “signing” contracts etc. And if it is set to “digital signature”, it is intended for authentication purposes only.

It has been argued that a key with a certificate marked “digital signature” should not be used to sign, or enter into, so-called “legally binding” instruments or transactions. The reason is that the authentication key might be used to sign so-called “challenges” (a random string of bits to be signed for authentication purposes) and the signer will not necessarily know what he is signing. Consequently, a “signature” based on an authentication certificate can more easily be disputed, with the signor claiming that he did not have an intention to be bound and that he did not know what he was signing. For the same reason, a certificate marked “non-repudiation” should not be used for pure authentication purposes. It would seem to be an open question whether or not it has any legal significance if the certificate is set for “non-repudiation” or “digital signature” when it comes to a concrete transaction.[19]

It is possible that this discussion has been brought to an end by the current ETSI certificate profile.[20] Pursuant to that profile, in cases where a certificate is intended to be used to validate commitment to signed content, such as electronic signatures on agreements and/or transactions, then the non-repudiation bit SHALL be set. Although not recommended, it might be set in combination with the digital signature bit. If the certificate is declared to be a Qualified Certificate according to TS 101 862, then the key usage bit shall be set to either non-repudiation or digital signature, or both of them in combination.[21]

2.4 Certification Services

We recall that a digital certificate is an electronic record that associates *eg* a given public key with an identifier. But how do we establish trust in this

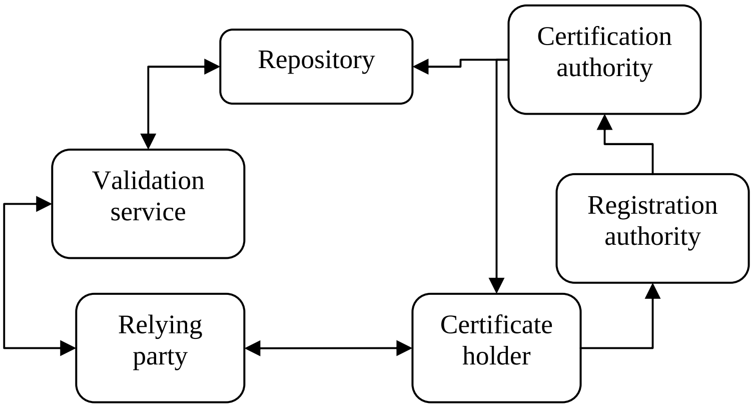
[19] Critical to this distinction is amongst others Winn, *see* Winn, Jane K., *The Emperors New Clothes: The shocking truth about digital signatures and internet commerce*, 37 Idaho L. Rev. 353 (2001). Revised draft March 9, 2001, available from “http://www.law.washington.edu/Faculty/Winn/Publications/The%20Emperor's%20New%20Clothes.htm”.

[20] ETSI TS 102 280, *X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons* (March 2004).

[21] *See* ETSI TS 102 280, para 5.4.3.

assertion? The commonly recognised solution is to let a certification service provider (CSP) sign the certificate. The “electronic signature” of the CSP will, in effect, render the certificate difficult to forge and, depending on the circumstances under which the certificate was issued, represent an attestation that the content of the certificate is correct. But this is not the whole truth. The signature of the CSP on the certificate may or may not imply that the CSP has undertaken a careful evaluation of the facts represented in the certificate. The level of control carried out by the CSP will usually appear from its certificate policy or similar statements. Another question is whether the CSP actually operates in accordance with its certificate policy.

Anyhow, regardless of the extent to which control measures are undertaken, and whether the CSP is trustworthy, a number of roles typically involved in a certification process can be identified as shown below.



A subject (potential certificate holder) applies for a certificate with a ‘registration authority’ (RA). The RA verifies the identity or attributes of the applicant and submits the data to the ‘certification authority’ (CA). The relevant data are generated and the certificate issued and signed by the CA and submitted to the certificate holder and to a ‘repository’. The keys involved might have been generated by the certificate holder or by the certification authority. Should a situation occur that would render the certificate invalid, revocation of the certificate would be registered with the repository. The RA, CA and the repository are commonly referred to as the ‘certification service provider’ (CSP). The CSP may be organised as one single organisation or the different roles may be undertaken by different organisations.

2.5 Certificate Valdation

Certificate validation is a process whose importance is much underestimated. Certificate validation is a complex process, the purpose of which is to establish a reasonable degree of confidence in whether or not a certificate can be trusted for a given transaction. This process, undertaken by the relying party, or on behalf of the relying party, is fundamental to establish trust in electronic signatures and digital certificates.

One may distinguish between certificate verification and certificate validation. During the verification process, a number of technical controls are undertaken. During the validation process, the certificate is tested for validity, *ie* that the certificate is not revoked, whether the certificate is suitable for the relevant transaction, etc. Information necessary to undertake such assessments may be collected from the repository as referenced in the relevant certificate. Careful validation of the certificate is relevant not only with regard to the trustworthiness of the certificate but even with regard to the question of CA liability for any misstatements.

Recommendations for *electronic signature* verification are found in Annex IV of the Electronic Signature Directive. These recommendations have not, in general, been implemented into Norwegian law. However, requirements for *certificate* verification, etc have been adopted in the Regulations on Electronic Communication with and within the Public Administration.[22]

3 Regulating Certification Services - the Electronic Signature Act

3.1 Implementing Directive 1999/93/EC

Electronic signatures and certification service providers that issue qualified certificates, are addressed by the Electronic Signature Directive.[23] The Electronic Signature Act implements the Directive into Norwegian law. Implementation of the Directive was subject to co-operation between the respective Ministries in each Scandinavian country, and similar acts have been adopted in the other Scandinavian countries.[24][25]

In addition to the Electronic Signature Act itself, further regulations regarding requirements for service providers issuing qualified certificates have been

[22] *See* Regulation of 25th June 2004, No 988 on Electronic Communication with and within the Public Administration, section 25 available (in Norwegian) at "http://www.lovdata.no/for/sf/aa/aa-20040625-0988.html".

[23] *See* more about the Directive 1999/93/EC in Dumortier, Jos, *The European Regulatory Framework for Electronic Signatures: A Critical Evaluation*, in Ruth Nielsen et.al. (eds.), EU Electronic Commerce Law, DJØF Publishing 2004, p. 69-93, *See* also Jos Dumortier, *Directive 1999/93/EC on a Community framework for electronic signatures*, in Arno R. Lodder and Kaspersen Henrik W.K. (eds.), eDirectives: Guide to European Union Law on E-Commerce, Kluwer Law International 2002, p. 33-65.

[24] *See* in Denmark Act No 417/2000 on Electronic Signatures and in Sweden Act (2000:832) on Qualified Electronic Signatures, both with further regulations.

[25] *See* more about the regulation in Sweden in *e.g.* Magnusson Sjöberg, Cecilia, *Elektroniska signaturer – ny lag men fortsatt behov av åtgärder*, Juridisk Tidskrift 2000-01, p. 864-882, and in Denmark in Udsen, Henrik, *Den digitale signatur – ansvarsspørgsmål*, Forlaget Thomson, København 2002.

adopted pursuant to the Act.[26] The Act and the regulations entered into force on 1st July 2001. A minor revision of the Act that includes, *inter alia,* a revised definition of an 'electronic signature' was adopted in December 2002 and entered into force on 1st January 2003.[27]

3.2 Scope and Area of Application

The scope of the Electronic Signature Act is to 'facilitate the secure and effective use of electronic signature by setting out requirements applicable to qualified certificates, to the issuers of such certificates and to secure signature creation devices' (section 1).[28]

The main issues of the Act are: 1) the legal recognition of electronic signatures, 2) requirements for so-called 'qualified certificates' and service providers issuing such certificates, 3) the supervision of such service providers, 4) requirements for so-called 'secure signature creation devices' and 5) the legal recognition of qualified certificates issued by service providers established outside Norway. A few of the provisions of the Act also apply to certificates that are not qualified certificates.

The Act applies to certification service providers established in Norway (section 2). It is not limited to certificates issued to the public but also applies to qualified certificates issued to so-called closed user groups. This appears to go beyond the scope of the Directive[29] and it is also contrary to the situation in Denmark and Sweden. The intention was to facilitate the widespread use of electronic signatures by ensuring better predictability with regard to the legal effect of signatures subject to the Act and its supervisory system. Moreover, it appears to be difficult to differentiate between certificates issued to the public and those issued to user-groups comprising a large number of participants.[30] Certificates from closed groups might also 'leak' out to an open environment. And when a service provider *chooses* to issue its certificates as qualified certificates, then the users will reasonably expect the certificates to be trustworthy. In this case, one might argue, that the certificate users should be protected by the liability regime of the Act, regardless of whether or not contracts are formed between the service provider and the users.

[26] *See* Regulation of 15th June 2001, no 611, on Requirements for Service Providers Issuing Qualified Certificates, hereinafter referred to as the 'Regulations on Qualified Certificates', available (in Norwegian) from "http://www.lovdata.no/for/sf/nh/nh-20010615-0611.html".

[27] The legislative history of the Act appears from Ot prp nr 82 (1999-2000) and Ot prp nr 103 (2001-2002), available (in Norwegian) from "http://odin.dep.no/nhd/norsk/publ/otprp/index-b-n-a.html".

[28] All translations from this and other acts are unofficial and undertaken by the author of this article.

[29] *See* recital 16 of the Directive which reads: '… a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; …'.

[30] *See* Ot prp nr 82 (1999-2000), para 7.2.3.

The Electronic Signature Act does not establish any *right* to use electronic communication. Whether or not electronic communication can be used, has to be decided on the basis of an interpretation of the law relevant to the area in question. Neither does it interfere with any other legal requirements as to form than requirements for signature. The Electronic Signature Act does not apply to the encryption of data for confidentiality purposes.

3.3 Definitions

a) Electronic signature

The term ’electronic signature’ was initially defined as ’data in electronic form which are related to other electronic data and which are used to control that those data originate from the one who appears to be the signer’. This definition limited the use of electronic signatures to physical persons only. The definition was later amended. The current provision reads: ’data in electronic form which are related to other electronic data and which are used as a method of authentication’ (section 3(1) in force from 1st January 2003). The reason for this adjustment was that ’signatures’ and authentication mechanisms used by automated systems or web-servers may be adequate and legally relevant and, consequently, the term electronic signature should not be limited to use by physical persons only.[31] This relates, for example, to the use of so-called ‘organisational certificates’ within the public administration, see below. As the Electronic Signature Act sets out general definitions, these should be wide enough to facilitate even other pieces of legislation.[32]

Like the Electronic Signature Directive, the Electronic Signature Act defines the term ‘advanced electronic signature’. The advanced electronic signature is an electronic signature that is a) uniquely linked to the signer; b) capable of identifying the signer; c) created using means that the signatory can maintain under his sole control; and d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[33]

A third ‘level’ of signature is the so-called ‘qualified electronic signature’. A ‘qualified electronic signature’ is an advanced electronic signature, which is based on a qualified certificate and generated by a secure signature creation device (section 3(3)).

b) Certificate

The term ‘certificate’ is defined as a link between signature verification data and a signer that confirms the identity of the signer and is signed by the certification service provider (CSP) (section 3(9)). Taking into consideration the definition of the term ‘signer’ in the Act, it probably means that the Act applies to identity certificates for physical persons only. Other types of certificates seem to be

[31] *See* Ot prp nr 103 (2001-2002), para 3.1 and para 5.

[32] *See* Ot prp nr 103 (2001-2002), para 3.1.

[33] *See* section 3(2)(a-d). The wording of para c) and d) is somewhat different from the text of the Directive, article 2(2). However, by interpretation, there should be conformity between the provisions. Consequently, the interpreted version is represented here.

outside the scope of the Act. This is the case also with regard to the term ‘qualified certificate’. However, as the reference to the ‘signer’ was removed from the amended definition of an electronic signature, such ‘signature’ may be generated by other than physical persons, *eg* from an automated system as mentioned above.

A qualified certificate shall contain information as defined in section 4 of the Act. It shall contain a statement that it is issued as a qualified certificate, the identity of the CSP and the country in which it is established. It shall also contain the name or a pseudonym of the signer (certificate holder) and other data about the signer to the extent that they are relevant for the use of the certificate. Furthermore, the certificate shall contain the signature verification data of the signer, the certificate’s validity period and identification number, the signature of the CSP and, if applicable, limitations with regard to the area of application or monetary limits for the transactions in which the certificate can be used. A certificate may only be issued as a qualified certificate when it is issued by a certification service provider that complies with the requirements of sections 10-15 of the Electronic Signature Act. The requirements of sections 4 and 10-15 correspond to Annex I and II of the Electronic Signature Directive.

In the Regulations on Electronic Communication with and within the Public Administration, an ‘organisational certificate’ is introduced.[34] The certificate associates the name of an administrative body with a public key. The intention is that the certificate shall be used to verify messages issued by the public administrative body. This is especially useful when a message originates from an automated system. But it has also been considered appropriate for other messages from the public administrative body. With regard to the citizens, the signature of a civil servant will not be very useful, as the citizens probably will not know the signer anyway. What matters for the citizen, is to be able to verify that a message really originates from, and is approved by, the public administrative body. As there is no general requirement for a handwritten signature to give legal effect to an administrative decision under Norwegian law, the authentication of the administrative body can more effectively be undertaken by way of organisational certificates.

c) Certification service provider

In the Electronic Signature Act, the service provider subject to the law is called the ’certificate issuer’[35]. The term is defined as ’a physical or legal person that issues certificates or provides other services related to electronic signature’. It is supposed to have the same broad meaning as the term ’certification-service-provider’ as used in the Electronic Signature Directive. This implies that, for example, directory services and time-stamping services, etc, in principle, are covered by the Act. In this article, the term ‘certification service provider’ (CSP) will be used, as it better reflects the area of application of the Act.

[34] *See* Regulation of 25th June 2004, No 988, on Electronic Communication with and within the Public Administration, section 14, available (in Norwegian) from “http://www.lovdata.no/for/sf/aa/aa-20040625-0988.html”.

[35] ‘Sertifikatutsteder’ in Norwegian, *see* section 3(10).

There are no general restrictions on providing certification services in Norway, neither is there any requirement for prior approval. However, while anyone can offer certification services, there are fairly detailed requirements for CSP's providing *qualified certificates*.

3.4 CSPs Providing Qualified Certificates

a) Registration

Any CSP established in Norway that wants to offer qualified certificates has to register with the Norwegian Post and Telecommunication Authority (NPT) prior to offering such services.[36] In connection with the registration, the CSP shall provide the NPT with information as described in the Regulations on Qualified Certificates.[37] Such information shall include *inter alia* the name and organisation number of the service provider, information on any agreements implying guarantees for the qualified certificates of other CSPs,[38] and a specification on how the requirement for financial resources have been complied with.[39] The CSP shall also provide the NPT with information on its certificate policy and certification practices, the routines for long-time recording of information relevant to the certificates,[40] the chosen IT-auditor if applicable, a copy of any model customer agreements, and information on any certifications held by the CSP. The NPT has developed a standard form for the registration.[41]

Information regarding the provision of qualified certificates shall be made publicly available by the NPT. Information on the routines for verification of identity pursuant to section 13 of the Electronic Signature Act, shall be collected and made available accordingly.[42] Amendments to existing registrations and new information to be registered shall be reported to the NPT without undue delay.[43] As at April 2003, only one company has registered with the NPT.[44]

b) Supervision

The Norwegian Post and Telecommunication Authority (NPT), has been appointed the supervisory authority pursuant to section 17 of the Electronic Signature Act,[45] cfr the Electronic Signature Directive art 3(3). The NPT shall supervise that CSPs that issue qualified certificates comply with the Electronic

[36] *See* the Electronic Signature Act, section 18.

[37] *See* the Regulations on Qualified Certificates, section 4 cfr section 2.

[38] *See* the Electronic Signature Act, section 25(2)(b).

[39] *See* the Electronic Signature Act, section 10(2).

[40] *See* the Electronic Signature Act, section 14.

[41] The form is available from "www.npt.no" (in Norwegian only).

[42] *See* the Regulations on Qualified Certificates, section 6 and 7.

[43] *See* the Regulations on Qualified Certificates, section 5.

[44] Zebsign, a company which is co-owned by Telenor and Norway Post, has registered itself with two different certificate policies; both related to identity certificates for individuals, *see* "www.npt.no" and "www.zebsign.no".

[45] *See* the Regulations on Qualified Certificates, section 8(1).

Signature Act and further regulations. The CSP shall pay a yearly fee to the NPT.[46]

The supervisory authority has been empowered with the right to require further information from the CSP,[47] to undertake controls at the CSP's premises,[48] and to require an IT-audit to be undertaken by the CSP.[49] The NPT has the right to instruct the CSP to take measures to correct divergences in order to comply with the Electronic Signature Act.[50] It may also impose daily fines.[51] Subject to material or repeated breach of the Act or Regulations by the CSP, the supervisory authority may exclude the CSP from the right to use the term 'qualified certificate'.[52] The CSP has the right to make a complaint to the Ministry of Trade and Industry against decisions made by the NPT pursuant to the Electronic Signature Act or the Regulations on Qualified Certificates.[53] So far, the supervisory activity has had a rather light-touch approach.

Some of the requirements of the law are subject to penal sanctions.[54] The penal sanctions comprise failure to register with the NPT pursuant to section 18, failure to give information pursuant to section 17, processing personal data contrary to sections 7 or 14, or providing misleading information to the supervisory authority.

c) Security and and procedural requirements

Certification service providers, issuing qualified certificates shall carry out their business in such a way that secure, reliable and well-functioning certificate services can be provided.[55] The CSP shall have sufficient economic resources to run the business in accordance with the requirements of the Act and its Regulations.[56] It shall use trustworthy products and systems, which are protected against modification and ensure the technical and cryptographic security of the processes supported by them.[57] Such requirements are considered to be complied

[46] *See* the Regulations on Qualified Certificates, section 9, cfr the Electronic Signature Act, section 24, and the Regulation on fees to the NPT. The fee in 2003 was NOK 100.000 (approx € 12500). The fee did not cover the cost incurred by the NPT for the supervisory activity. Nevertheless, due to the market situation, the NPT, under agreement with the Ministry of Trade and Industry, has decided not to claim any yearly fees related to this service in 2004 and 2005.

[47] *See* the Electronic Signature Act, section 17(2), and the Regulations on Qualified Certificates, section 8(2).

[48] *See* the Electronic Signature Act, section 19, and the Regulations on Qualified Certificates, section 8(3).

[49] *See* the Electronic Signature Act, section 17(4).

[50] *See* the Electronic Signature Act, section 17(3).

[51] *See* the Electronic Signature Act, section 20, and the Regulations on Qualified Certificates, section 10(1).

[52] *See* the Electronic Signature Act, section 17(5), and the Regulations on Qualified Certificates, section 10(2).

[53] *See* the Regulations on Qualified Certificates, section 12, cfr the Public Administration Act.

[54] *See* the Electronic Signature Act, section 21.

[55] *See* the Electronic Signature Act, section 10(1).

[56] *See* the Electronic Signature Act, section 10(2).

[57] *See* the Electronic Signature Act, section 11.

with when the products and systems used by the CSP either have been approved by an organisation appointed pursuant to section 9, or comply with standards approved by the European Commission and published in the Official Journal of the European Communities.[58] Such specifications have been provided.[59]

The CSP shall take precautions against forgery of the certificates and ensure the confidentiality of signature-creation-data if they are generated by the CSP.[60] The CSP shall not record or copy the signature-creation-data of the signer.[61]

A prompt and secure directory and revocation service shall be provided by the CSP. The CSP must ensure that the date and time when a certificate comes into force or is being revoked may be determined precisely.[62]

The identity of the signer and other relevant data shall be verified by secure routines.[63] Information on said routines shall be publicly available.[64] It appears from the Regulations on Qualified Certificates that the identity of the signer, as a general rule, shall be verified by way of physical presence with the CSP or its representative. Exception is made if the signer has been identified by physical presence during an existing relationship.[65]

All relevant data regarding qualified certificates shall be archived for a reasonable period of time but for a minimum of 10 years following the time of registration in a revocation list (or expiry of the certificate).[66] CSPs issuing qualified certificates shall also have procedures to handle the situation where the business closes down, *ie* to ensure the recording and accessibility of certificates and other relevant information.[67] The CSP shall use reliable systems to record the certificates such that the authenticity of the data can be verified and that any changes compromising the security requirements are apparent to the operator.[68]

Prior to entering into agreements to issue a qualified certificate, the CSP shall inform the other party about the terms and agreements regarding the use of the certificate, and provide information on the existence of any voluntary accreditation or certification schemes and the procedures for complaints and dispute resolution.[69] Said information may be submitted electronically but must be in writing and in a readily understandable form. The information shall also be available to the relying party.[70]

[58] In Denmark and Sweden, assessment of secure signature creation devices by a designated body is mandatory.

[59] *See* Commission Decision 2003/511/EC of 14 July 2003 (OJ L 175, 15.07.2003, p. 45).

[60] *See* the Electronic Signature Act, section 11.

[61] *See* the Electronic Signature Act, section 14, last sentence.

[62] *See* the Electronic Signature Act, section 12.

[63] *See* the Electronic Signature Act, section 13(1).

[64] *See* the Electronic Signature Act, section 13(2).

[65] *See* the Regulations on Qualified Certificates, section 7, cfr the Electronic Signature Act, section 13.

[66] *See* the Electronic Signature Act, section 14(1).

[67] *See* the Regulations on Qualified Certificates, section 3, cfr the Electronic Signature Act, section 14.

[68] *See* the Electronic Signature Act, section 14.

[69] *See* the Electronic Signature Act, section 15(1).

[70] *See* the Electronic Signature Act, section 15(2).

d) Liability

Certification service providers are subject to national rules regarding liability.[71] However, certain minimum requirements appear from article 6 of the Electronic Signature Directive, applicable to CSPs that issue qualified certificates. These requirements have been implemented in section 22 of the Electronic Signature Act. The liability is based upon negligence with a reversed burden of proof. Broadly speaking, a certification service provider that issues qualified certificates is liable for damage caused to any party who reasonably relies on the content of such certificates as regards the accuracy of their content at the time they were issued, their compliance with section 4 of the Act and for failure to register the certificate in a revocation list, unless the provider proves that he has not acted negligently. The CSP is not liable to the extent that the certificates have been used contrary to any limitations regarding the use of the certificates or any monetary limits, provided that such limitations are easily recognisable by third parties.

3.5 Data Protection

To the extent that the certification service provider processes personal data, the certification service is subject to the Personal Data Act.[72] The certificate service provider must also comply with section 7 of the Electronic Signature Act regarding the collection and processing of personal data. This provision applies to all certificates as defined by the Electronic Signature Act and is not limited to qualified certificates only.

Section 7 lays down three requirements. Firstly, data about a person may only be collected from the person himself, or subject to the explicit consent of the person. Secondly, data can only be collected to the extent that it is necessary in order to issue or maintain a certificate. Thirdly, the data cannot be used for any other purpose, unless the person has given his explicit consent to do so.

If the certificate is a qualified certificate, it shall not be made publicly available unless the holder of the certificate has given his consent.[73] It does not appear from the Electronic Signature Act why this provision addresses qualified certificates only.

The Data Inspectorate shall superintend that section 7 of the Electronic Signature Act is complied with. The supervisory activity of the Data Inspectorate is subject to the procedures of sections 42-47 of the Personal Data Act.[74]

[71] *See* the Electronic Signature Directive recital 22.

[72] Act of 14th April 2000, No 31, relating to the processing of personal data (Personal Data Act).

[73] *See* the Electronic Signature Act, section 14(2)(b).

[74] *See* the Electronic Signature Act, section 7(2).

3.6 Legal Recognition of Certificates Issued by a CSP Established Outside Norway

Certificates issued by a CSP established within another country in the EEA area are considered to be qualified certificates pursuant to the Electronic Signature Act, provided that they comply with the requirements for such certificates in their country of origin (section 25(1)).

Qualified certificates, which are issued by a CSP established outside the EEA area shall be subject to the same legal recognition as certificates issued within the area, provided that the issuer complies with the requirements of an EEA state and has been accredited under a voluntary accreditation scheme in that state; or a CSP established within the EEA area, that complies with the requirements of the state in which it is established, guarantees the certificate; or the certificate or the CSP is recognised under an agreement between Norway or the EU and a third country or an international organisation (section 25(2)).

3.7 Legal Recognition of Electronic Signatures

The term 'electronic signature' is rarely used in Norwegian legislation. It occurs in a few acts and regulations only, in addition, of course, to the Electronic Signature Act itself. More surprising, perhaps, is that the number of provisions containing the term 'signature' and which are relevant to the use of electronic communication, are relatively small. However, other requirements as to form might be relevant.

There is no general legal definition of the term 'signature' under Norwegian law. Neither is there any common understanding of how a requirement for signature should be interpreted when applied to electronic communication. It will depend on the area of law and the rationale of the requirement in question.

Even though it has not been tested in court, electronic signatures seem to be widely accepted as an adequate method of authentication in areas of law where electronic communication is permitted, see section 4 below.

Article 5 of the Electronic Signature Directive deals with the legal recognition of electronic signature. It has been implemented in Norwegian law through the Electronic Signature Act. It appears from section 6 that 'if, in a law, regulations, or in any other way, there is a requirement for signature in order to obtain a certain legal effect, and the transaction can [legally] be performed by electronic means, a qualified electronic signature shall always be deemed to comply with such requirement'. A qualified electronic signature is an advanced electronic signature, based on a qualified certificate and generated by a secure signature creation device.

For other electronic signatures, *ie* signatures that are not qualified electronic signatures, the Electronic Signature Act might seem to deviate from the Electronic Signature Directive. In the Directive, it is stated that such electronic signature shall not be denied legal effect, solely on the grounds that it is in electronic form or because it is not based on a qualified certificate etc (art 5(2)). While the Electronic Signature Act simply states, with reference to the legal effect of qualified electronic signatures, that other electronic signatures *may* have such legal effect (section 6, last sentence). No further directions are given. Hence, the legal effect of such electronic signatures has to be assessed on an individual basis, taking into consideration the kind of signature and the legal requirement in question. However, in practice, and by interpretation, the Act is not expected or intended to give other results than those foreseen by the Directive.[75]

4 Other Legal Framework Facilitating Electronic Communication and Certification Services

There are presumably few legal obstacles towards the use of public key technology. Exporting encryption technology is subject to export restrictions under the so-called "dual goods" regulations issued pursuant to the Wassenaar Arrangement. However, these regulations have recently been revised and do not represent an obstacle to the use of "off-the-shelf" public key encryption technology for commercial purposes.

4.1 Law Reforms - 'eRegelprosjektet' etc

In order to further meet the requirements for a regulatory regime which is facilitating electronic commerce and communication, a major law reform, called the 'eRegelprosjektet'[76], was launched in 2000. The project was based on a survey of Norwegian law,[77] with the aim of identifying provisions of law that might represent an obstacle to electronic communication. As a result of the 'eRegelprosjektet', proposals for amendments to 39 different Acts from different areas of law were collectively presented to the Parliament as one common Bill,[78] and was adopted in December 2001.[79]

Among the provisions amended were requirements for signature and other requirements as to form. Even though such provisions did not in all cases represent an obstacle to electronic communication, some of them were amended to prevent confusion on whether or not the paper form or a handwritten signature was required. One of the techniques used was to replace requirements for signature or to supplement other provisions as to form, with a requirement to use 'a secure method to authenticate the originator (or the contract formation)' and/or to 'secure the content of the communication/agreement'.[80] Electronic signatures and certification services may comply with these requirements.

The requirement for a message or communication to be in 'writing' is now regularly interpreted such as to include electronic communication. This interpretation has in some areas of law been formalised, for instance in the

[75] Se Ot prp No 82 (1999-2000), para 8.10.2.

[76] The name may be interpreted as the 'eLawProject'.

[77] The so-called 'Kartleggingsprosjektet' undertaken 1999-2000.

[78] *See* Ot prp No 108 (2000-2001) and Ot prp No 9 (2001-2002).

[79] A similar project has been undertaken in Denmark, *see* "http://e.gov.dk/formkrav".

[80] *See e.g.* the Credit Sales Act 1985 No 82 (Kredittkjøpsloven), section 3a.

Public Administration Act. The requirement for writing is defined there as "also [an] electronic message, provided that the information is accessible even in the future".[81] In most cases, however, it is a requirement that the parties, or at least the receiver, has explicitly agreed to use electronic communication.[82] As a curiosity, it is worth mentioning that this interpretation has become so common, that in some cases where the paperform should be retained, one found it necessary to re-phrase certain requirements in the Acts, such that they now read 'in writing on paper', in order to avoid confusion.[83]

The question of electronic communication with the courts, and registration of title to land, etc, was not included in the eRegelprosjektet. However, this was addressed by a bill adopted in April 2003.[84] Once the amendments to the legal procedure legislation enter into force, further regulations may be adopted by the Government addressing when, and under what conditions, electronic communication with the courts and registries can take place. Such provisions may contain requirements for security services such as electronic signatures, encryption and certification services.

4.2 Public Sector Regulations

Communication in the public sector is in general dealt with by the Public Administration Act,[85] which also applies to electronic communication. Further Regulations on Electronic Communication with and within the Public Administration were adopted in 2002. New regulations (commonly called 'eForvaltningsforskriften') were adopted on 25th June 2004 and entered into force on 1st July 2004.[86]

The regulations requires all public administrative bodies, which engage in electronic communication, to establish a security policy. The security policy shall address, among other things: whether, when and how to use security services, including electronic signatures, encryption and related certification services (see section 13, cfr section 4, of the regulations). To the extent that encryption and certification services are being used, section 14 to 26 of the regulations apply, addressing issues such as: requirements for organisational certificates, requirements to inform about security services, safekeeping of

[81] In Norwegian: "skriftlig: også elektronisk melding når informasjonen i denne er tilgjengelig også for ettertiden". *See* the Public Administration Act, section 2(g).

[82] *See e.g.* the Public Administration Act, sections 16 and 27.

[83] *See e.g.* the Debt Collection Act 1988 No 26 (Inkassoloven), sections 9 and 10 regarding notice concerning collection of debts, the Securities Trading Act 1997 No 79 (Verdipapirhandelsloven), section 5-11, and special parts of the company legislation, *e.g.* the Partnerships Act 1985 No 83 (Selskapsloven), sections 2-30 and 2-35.

[84] *See* Act on Amendments to the Legal Procedure Legislation etc (Electronic Communication with the Courts etc) of 25th April 2003, No 24 (not yet in force as at April 2004).

[85] The Public Administration Act of 10th February 1967.

[86] Regulations 25th June 2004 No 988 on Electronic Communication with and within the Public Administration adopted pursuant to the Public Administration Act, section 15a and the Electronic Signature Act, section 5.

signature-creation-data and decryption keys, requirements for signature verification, long term recording of electronic signatures, etc.

One will of course also find sector specific regulation, *eg* in the health care sector.

The Electronic Signature Directive foresees, and permits, the possible need for more specific regulations on the use of electronic signature in the public sector (art 3(7)). Pursuant to section 5 of the Electronic Signature Act, such additional requirements can be adopted by way of further regulations (secondary legislation). Even though the Regulations on Electronic Communication with and within the Public Administration contain a reference to said provision, and do indeed contain provisions related to electronic signatures, no *additional* requirements for electronic signatures, as such, have been adopted as yet (April 2004).

During the last years, requirements and framework agreements for certification services and other IT-services for the public sector were, to a certain extent, co-ordinated through a joint acquisition project, the so-called 'Forvaltningsnettsamarbeidet'. The project was terminated ultimo 2002. However, there is an obvious need to continue the co-ordination in this area.

It appears from section 28 of the Regulations on Electronic Communication with and within the Public Administration that a co-ordinating body may be appointed. Such body shall co-ordinate the use of information security services in the public sector. To obtain this, the co-ordinating body shall develop requirements for security services and products that are recommended for electronic communication. The co-ordinating body shall asses whether products and services available in the market comply with the requirements. The co-ordinating body may also decide that public administrative bodies, if certificates are being used, shall use service providers that have entered into framework agreements with the public administration or providers that are recognised by the co-ordinating body. Such co-ordinating body was established in January 2004. The mandate of the co-ordinating body is, however, less extensive than prepared for by the regulations. The main objective of the co-ordinating body, is to facilitate trust in electronic communication by encouraging co-ordinated use of electronic IDs and electronic signature in communications with the public sector.[87] According to the IT-policy of the Norwegian Government (eNorge 2005), the target is that "Conditions shall be established by the end of 2005 ensuring the general public access to standard-based electronic signatures".[88]

[87] *See* "http://odin.dep.no/aad/modernisering/tverrgaendeprosjekter/pkiorgan/index-b-n-a.html."

[88] *See* eNorge 2005, para 2.3, available from "http://www.enorge.org/".