# A EUROPEAN VIEW TOWARDS THE LEGAL RECOGNITION OF ELECTRONIC SIGNATURES IN NORWAY

A comparison between Art. 5 Electronic Signatures Directive and Section 6 Electronic Signatures Act in Norway

Candidate number: 6

Supervisor: Dr. Rolf Riisnæs

Deadline for submission: 12/15/2009

Number of words: 17,995 (max. 18.000)

03.12.2009

# Content

# 1 Introduction

In different jurisdictions the growing use of online facilities has been taken into account. The Norwegian government has the goal of deepening the acceptance, trust building and legal certainty of electronic communication in the same way as traditional written communication because electronic communication is used more and more.[1] Electronic communication should fulfil the legal requirements set up in different laws for communication.[2] Electronic communication should have a broad understanding and should be applied to all sorts of electronic cooperation.[3] This should lead not to a duty to use electronic communication means but to develop coexistence between electronic and paper-based communication.[4] One of these attempts to equate electronic communication with paper-base communication is the equation of handwritten and electronic signatures. The technology which was developed to fulfil similar functions of a handwritten signature is called electronic or digital signatures. The Electronic Signatures Directive (ESD) and its Norwegian implementation contains in Art. 5 ESD and Section 6 Norwegian Electronic Signatures Act (ESA) rules which say that electronic or digital signatures should be equalised with a handwritten signature.

## 1.1 Subject

This thesis asks the question if the Section 6 Norwegian Electronic Signatures Act (ESA) implements Art. 5 Electronic Signature Directive (ESD) correctly because there are some differences between Section 6 ESA and Art. 5 ESD. They will be discussed in this thesis under the focus of whether Section 6 ESA complies with Art. 5 ESD or not. To discuss the implementation thorough not only the two regulations have to be compared because some requirements of both regulations are defined in other regulations. In the first four chapters the very similar requirements for both laws will be described and compared. Beneath a general

[1] Ot.prp.nr. 108 (2000-2001), p. 3.
[2] Ot.prp.nr. 108 (2000-2001), p. 3.
[3] Ot.prp.nr. 108 (2000-2001), p. 3.
[4] Ot.prp.nr. 108 (2000-2001), p. 4.

chapter the technological requirements of Art. 5 I ESD and Section 6 ESA will be discussed in one chapter. Although some of these requirements such as advanced electronic signatures, qualified certificates, certification service providers and secure-signature-creation devices are regulated in other provisions, it is necessary to compare them as well. If they do not resemble the technical background Art. 5 ESD and Section 6 ESA will not comply with each other. This can result in different sorts of electronic signatures Art. 5 ESD and Section 6 ESA affect. Then the consequences of the Norwegian implementation will be discussed under the focus of the EFTA-Court legislation. Because of some legislation of the EFTA-Court is based on decisions of the ECJ, the necessary ECJ-decisions will be discussed as well.

## 1.2 What might electronic signatures be useful for?

A lot of communication is done electronically today, for example within a company employees usually use E-Mails or other electronic means to communicate with each other, contract drafts are exchanged via E-Mail. An electronic signature should fulfil the same functions as a handwritten signature to reach the same legal recognition. A handwritten signature has got different functions[5]:

- Data authority authentication
- Integrity
- Non-repudiation
- Verification
- Forgery
- Link between authentication tool and content
- Verifiable as long as the legal act is of legal importance
- Secure Date

Although a handwritten signature often does not fulfil these functions technically because it is relatively easy to copy while verification is difficult if the real and verified signature is missing.[6] If an electronic signature can fulfil these functions like a handwritten signature does, it can take over as an electronic substitute of a handwritten signature.

The same evidential weight as handwritten signatures should also be granted to electronic signatures before court to avoid the following. Often the electronic communication between two parties is printed out and given as evidence before court.[7] The problem with these prints can be that a manipulation of an electronic document is hardly detectable[8] and a later change of the document is claimed before court by one of the parties. Another point to consider is that it might be more convenient to give evidence in an electronic form. The question of subsequent changes can be a crucial point before court if the content of a contract is discussed. Most judges and

[5] Dumortier, The Legal Aspects of Digital Signatures, Vol. II, p. 54 f.
[6] Dumortier, The Legal Aspects of Digital Signatures, Vol. II, p. 56.
[7] Thorvaldsen, Skomedal, Ericson, Bevisverdien av elektronisk informasjon, Revisjon og Regnskap, 4/2007, p.1
[8] Thorvaldsen, Skomedal, Ericson, Bevisverdien av elektronisk informasjon, Revisjon og Regnskap, 4/2007, p.1.

lawyers do not have the knowledge to detect changes in electronic documents. Even for experts it is very difficult to detect manipulations of electronic communications. Therefore the parties have the obligation to use secure electronic means if they communicate electronically. One of a possible method to do this is the use of digital or electronic signatures. Especially electronic signatures that are based on a PKI are capable of detecting changes within the electronic communication.

Electronic signatures are also a means to authenticate the senders.

To ensure that judges do not reject electronic documents as evidence and to hinder establishing a barrier in the use of electronic communications the EU-Commission decided to give rules for the legal recognition of electronic signatures which has to be implemented within all Member States of the EU and all EEA-States. The only problem with the equivalence with a handwritten signature is that electronic signatures can prove something more than a handwritten signature does, because the technology producing digital signatures can also be used for other purposes.[9] But ESD and ESA do not exclude the use of other functions of electronic signatures technology because both laws take only one specific function, the signing function, the technology can have. Other authentication methods or cryptographic functions of the technology are not affected by these regulations.

[9] Dumortier, The Legal Aspects of Digital Signatures, Vol. VI, p. 31.

## 1.3 Technology

As the way in which electronic signatures work can be difficult to understand I will give a general overview of how the systems work. The ESD and the ESA deal with three different sorts of signatures: an electronic signature can be every electronic data that authenticates someone if it is attached to an electronic document.[10] In terms of information security authentication can be defined as data origin authentication, integrity of contents and non-repudiation of the author.[11] Some say that this can be everything from a typed name under an E-Mail[12] or a scanned handwritten signature[13] to a more sophisticated use of a simple encryption signature.[14]

Although these methods to authenticate do not cover perfectly all requirements the definition of authentication presumes, these methods can serve those functions.

Encryption technology is used to 'sign' an electronic document. The advanced electronic signature is said to describe so-called digital signatures which are based on encryption technology. The general principle can be described as a reverse use of encryption keys. There are two different systems of encryption used today. One is the symmetric or private key encryption and the other is the asymmetric encryption or public key encryption.[15]

If one uses a private key encryption both parties encrypt and decrypt with the same key.[16] The disadvantage of this system is that both parties have to know the key to decrypt and encrypt in advance[17]. The crucial point is the key exchange mechanism so no intruder can gain the key. Then the intruder is not able to impersonate one of the parties.[18] The risk can be reduced by using a key only once but this solution seems to be rather impractical.[19] If a private key

---

[10] See definitions Art. 2 (1) ESD, Section 3 (a) NESA.
[11] Dumortier, The Legal aspects of Digital signatures,Vol. II, p. 52.
[12] Mason, Electronic Signatures in Law, p. 280; Dumortier, The Legal aspects of Digital signatures, Vol. I, p. 8.
[13] Dumortier, The Legal aspects of Digital signatures, Vol. I, p. 8.
[14] Dumortier, The Legal aspects of Digital signatures, Vol. I, p. 8.
[15] Brazell, 3-037; Dumortier, The Legal aspects of Digital signatures,Vol. II, p. 25; Nordén Electronic Signatures in a legal context, 8.2.1; Reed, What is a signature, 4.3.
[16] Brazell, 3-037; Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 25; Nordén Electronic Signatures in a legal context, 8.2.1; Reed, What is a signature, 4.3.
[17] Brazell, 3-037; Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 25; Nordén Electronic Signatures in a legal context, 8.2.1.
[18] Brazell, 3-037.
[19] Brazell, 3-037.

encryption is used for signing a message the problem arises if a non-repudiation function is not obtained.[20]

More secure is public key encryption. Each party has two keys: one public and one private key.[21] For encryptions purposes the keys are used as followed: to encrypt a message the message must be encrypted with the public key and decrypted with the private because that ensures the secrecy of the message.[22] The public key can published without the security a private key needs as the private key is only used for decryption and the public key only for encryption.[23] The decryption without the appropriate key is usually difficult within such a system because the public key algorithm usually uses difficult mathematical problems to generate the keys.[24] The advantage of this system is that the private keys must not be exchanged.[25] Therefore it is difficult for an intruder to find out what the private key is and to impersonate one of the key-holders.

This technology can be used as signing means for an electronic document if it is used in a reversed way than in the encryption purposes.[26] The private key is then used for encryption and the public key for decryption.[27] To sign an electronic message three steps have to be taken

- 1. Produce a unique thumbprint of the message. This thumbprint is often a hash value that is a fixed-sized number derived from the electronic message that should be signed. This value is unique for every message.[28]
- 2. The hash value is then encrypted using the private key of the user and the encrypted hash value is attached as string of data to the message.[29]
- 3. The receiver of the message decrypts the hash value with the public key, generates a second hash value with the public key and compares the two hash values.[30]

---

[20] Electronic Signatures in a legal context, 8.2.1.
[21] Brazell, 3-037; Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 25; Nordén, Electronic Signatures in a legal context, 8.2.1; Riisnæs, p. 56.
[22] Feghhi, Feghhi, Williams, Digital Certificates, p. 37 f.
[23] Brazell, 3-037; Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 25; Nordén, Electronic Signatures in a legal context, 8.2.1.
[24] Brazell, 3-037; Feghhi, Feghhi, Williams, Digital Certificates, p. 37 f.
[25] Brazell, 3-037.
[26] Brazell, 3-040.
[27] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 30 f; Nordén, Electronic Signatures in a legal context, 8.2.1.
[28] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 30 f; Nordén, Electronic Signatures in a legal context, 8.2.1.
[29] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 30 f; Nordén, Electronic Signatures in a legal context, 8.2.1.

This shows two things:[31] The receiver can verify that the hash value has been encrypted with the sender's private key and that the message has not been altered because every alternation of the message produces another hash value.[32]

Such a system can look like this: often smart cards are used to sign an electronic document. The signature creation data can be stored on a PC or on an USB-device. Usually a smart card is used to store the private key on it. In general the hash value is send to the smart card which generates then the encrypted hash value and returns it back.[33] The advantage smart cards have is that they can not be tampered with, that means it is not possible to read the stored information without the password or by physical means such as deriving the information from the processor by studying the structure.[34] There are different smart card systems available.[35]

---

[30] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 30 f; Nordén, Electronic Signatures in a legal context, 8.2.1.
[31] Brazell, 3-040.
[32] Nordén, Electronic Signatures in a legal context, 8.2.1.
[33] Schellekens p. 51.
[34] Schellekens p.51f.
[35] For a detailed description of the different systems see http://www.smartcardbasics.com/cardtypes.html; visited 21.07.2009.

## 2 General Description of Art. 5 ESD and Section 6 ESA

Both laws set up rules for legal recognition of electronic signatures. As the Norwegian Law is an implementation of the ESD a lot of things are alike and can be found in both laws. In a very general way both laws have the same approach towards the regulation of electronic signatures. Both can be parted into two parts which deals with the legal recognition of different sorts of electronic signatures. This approach is called a two-track approach[36] because it ties two different levels of legal recognition together in one regulation. With this approach the legislator tries to give a minimum recognition for all sorts of electronic signatures and a legal certainty to specific technology. Both laws combine a minimalist approach and a prescriptive approach.

### 2.1 Art. 5 ESD

Art. 5 ESD divides the legal recognition of digital signatures into two parts. Part one gives the same legal recognition to a so-called qualified signature[37] in relation to an electronic document in the same manner a handwritten signature in relation to a written document does. In this part qualified signatures are as well admissible as piece of evidence as a handwritten signature. Part two is a non-discrimination rule for electronic signatures in general. This approach is called a two-track approach[38] because it ties two different classes of legal recognition together in one regulation:

- Track 1: the simple electronic signature cannot be discriminated just because it is electronic and/or not a qualified signature,
- Track 2: the qualified signature has to be recognized as equivalent with a handwritten signature and is admissible as piece of evidence.[39]

---

[36] Bell, Gomez, Mayer-Schönberger, Electronic Signature Regulation, CLSR, Vol. 17, 399 (401).
[37] Sjöberg, Nordén, Managing electronic Signaturs, fn. 11; Dumortier, The Legal and Market Aspects of Electronic Signatures, p. 150.
[38] Bell, Gomez, Mayer-Schönberger, Electronic Signature Regulation, CLSR, Vol. 17, 399 (401).
[39] Bell, Gomez, Mayer-Schönberger, Electronic Signature Regulation, CLSR, Vol. 17, 399 (400).

With this structure the EU implemented a two-tiered approach, which combines a minimalist approach and a prescriptive approach.[40] The minimalist approach contains only a non-discrimination rule for electronic-signatures like that one in Art 5 II ESD.[41] The prescriptive approach mandates the functions of one specific technology it describes in the law.[42] This is done in Art. 5 I ESD in which an advanced electronic signature must be based on a qualified signature and must be created by a secure signature-creation-device to gain equivalence with a handwritten signature and to be admissible as a piece of evidence. Art. 5 ESD shows a high flexibility because it gives legal certainty to a certain type of electronic signatures and ensures a minimum recognition for all forms of electronic signatures.[43]

[40] Wang, Critical review, CLSR, Vol. 23, 32 (33-36).
[41] Wang, Critical review, CLSR, Vol. 23, 32 (33).
[42] Wang, Critical review, CLSR, Vol. 23, 32 (34); Kuner, ILPF working paper, on: http://www.ilpf.org/groups/analysis_IEDSII.htm, visited: 24.11.2009.
[43] Wang, Critical review, CLSR, Vol. 23, 32 (36).

## 2.2 Section 6 ESA

Section 6 of the Norwegian Electronic Signatures Act (ESA) deals with the legal recognition of electronic signatures. In the Norwegian Law the two-tier approach is found as well. This approach is again displayed in the structure of the Section: the Section consists of two sentences. The first sentence contains the legal recognition of a qualified signature. The second sentence contains a legal recognition of an electronic signature as a basic rule. The first sentence deals with a high-technology solution that shall be equal to a handwritten signature. Section 6 S. 1 of the Norwegian ESA contains the legal recognition of a qualified signature. It says that if in a law or regulation or in any other means a requirement is laid down for signatures in order to obtain a specific legal effect and the provision may be implemented electronically, a qualified signature shall in every case meet such a requirement.[44] The second sentence has an approach for low technology solutions or technology solutions that does not fulfil all requirements of a qualified signature that might be equal to a handwritten signature. The prescriptive approach can be found in the first sentence where a certain technology is getting equivalence with a handwritten signature. The second sentence represents the minimalist approach because every electronic signature can gain a certain legal recognition. Again the Norwegian law shows the same flexibility like the Directive.

[44] Unofficial translation by http://www.npt.no/ikbViewer/Content/1379/1379-electronic_signatures_act.pdf; visited 23.07.2009.

# 3 Qualified Signature

This subchapter will first explain which requirements an electronic signature has to fulfil according to Art. 5 I ESD and Section 6 S. 1 ESA to be a qualified signature. In this work a qualified signature will be defined as an advanced electronic signature based on a qualified certificate and which is created by a secure-signature-creation device. [45]

## 3.1 Advanced electronic signature

An advanced electronic signature is defined in Art. 2 (2) ESD and Section 3 No. 2 ESA as an electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The technique thought to fulfil this definition is a type of asymmetric cryptography.[46] The requirements are fulfilled by signatures which are based on a PKI system using the RSA-algorithm.[47]

### 3.1.1 Uniquely linked to the signatory

As the private key and the public key belong together a signature shows that the message has been signed with the private key that belongs to the public key.[48] It is therefore possible to identify the private key with this system.[49] If someone knows that the sender owns the private key and knows beyond all doubt that the private key is not revealed and used by third persons or

---

[45] Art. 5 I ESD, Section 6 NESA, Unofficial translation by http://www.npt.no/ikbViewer/Content/1379/1379-electronic_signatures_act.pdf; visited 23.07.2009.
[46] Brazell, 5-033.
[47] Feghhi, Feghhi, Williams, Digital Certificates, p. 38.
[48] Brazell, 3-041.
[49] Brazell, 3-041.

lost by the sender one can identify with this method the sender of the message.[50] A problem is if the link between the two keys can be extended to the owner of the keys. Some argue that this is not the case because no one is capable to memorise a key due to its complexity.[51] But in the real world the key will be stored on some storage device, for example in computer memories, floppy disks or smart cards.[52] Therefore others argue that the requirement of Art. 2 (2) a) ESD/ Section 3 No. 2 ESA must be interpreted to mean a unique logical link between the signature and the signatory.[53] For this interpretation the third requirement in Art. 2 (2) c) ESD should also speak because it explicitly allows storage devices.[54]

The second argumentation has an important point because all storage devices are possessed. In some legislation possession gives the presumption for ownership.[55] This means for storage devices that the person who possesses the device is the owner. The problem is, if one can presume that the data on the storage device also belongs to the possessor and owner of the storage device. This can be still doubted. Therefore the argumentation that the possession of a storage device helps to establish a unique link between electronic signature and the signatory does not help. I think this link can only be established if one can make the presumption that a key holder usually does not reveal his private key to others. But this presumption can only be established if the time has proved this. The German Bundesgerichtshof takes that view in its decision XI ZR 210/03. The judges presume that if the right PIN is used when someone takes cash from an ATM the bank account holder took that money[56]. The judges think therefore that there is a unique link between PINs and bank account holders. A reasoning of this presumption can be found in decision 9 U 63/01 of Oberlandesgericht Stuttgart. The judges think that the PIN is delivered to the customer and secured in a way so that it is not possible that a third person can retrieve the data from the bank via manipulations or guess the PIN by a brute force attack. The only way according to these courts to get knowledge of the PIN is if the holder of the PIN is acting negligently. This means for the technology as such, the PIN is uniquely linked to the bank

[50] Feghhi, Feghhi, Williams, Digital Certificates, p. 46.
[51] Mason, Electronic Signatures in Law, p. 148; Brazell 5-046.
[52] Brazell 5-046.
[53] Brazell 5-046.
[54] Brazell 5-046.
[55] See Section 1006 BGB.
[56] BGH, XI ZR 210/03, p. 11; Kindl/Werner CR 2006, 353 (359).

account holder. Therefore one have to say for now that the requirement of an unique link between electronic signature and signatory exists only if the private key is hold secret so only the signatory can use it.

### 3.1.2 Capable of identifying the signatory

It is possible to identify the private key within a PKI-system because the private key and the public key are linked together.[57] If someone knows that the sender owns the private key and knows beyond doubts that the private key is not revealed and used by third persons or lost by the sender one can identify via that link with this method the sender of the message.[58]

### 3.1.3 Created by means under sole control of the signatory can maintain

But the sender of the message has to exercise a sort of sole control over means that creates the signature. The above mentioned criterion of secrecy is taken over with the requirement "sole control". This creates a problem because the recipient of a message signed with a private key cannot know if the private key is under the 'sole control' of the sender if it is located on a computer or stored on a smartcard.[59] The sender does not know who has access to the key data if the private key is stored on a computer or, if stored on a smartcard, the recipient does not know who is using the smartcard because it might be borrowed or stolen.[60] According to a working paper of the FESA it is part of the nature of a digital environment that the signatory needs a comprehensible version of a security concept and confidence that the service provider sticks to the security concept.[61]Therefore the sender has to use some security measures to maintain sole control.[62] With a good security concept a signatory can have even within a server-based system sole control over the private key argues the working paper.[63] But there is room to argue that sole control implies a physical control about a thing because this question is dealing with the definition of sole control. Physical control is impossible to establish within a server based system that creates signatures because the data is not attached to a physical device. Therefore a server

[57] Brazell, 3-041.
[58] Feghhi, Feghhi, Williams, Digital Certificates, p. 46.
[59] Mason, Electronic Signatures in Law, p. 149.
[60] Mason, Electronic Signatures in Law, p. 149.
[61] Working Paper, found on Mason, Electronic Signatures in Law, p. 150.
[62] Mason, Electronic Signatures in Law, p. 149.
[63] Working Paper, found on Mason, Electronic Signatures in Law, p. 150.

based system is not able to create sole control over the means that create the signature.[64] This means that sole control has got a physical component that has to be taken into account. Otherwise the meaning of 'sole control' is being distorted.[65] Sole control means therefore a physical power over the signature creation data which means one person is in charge to decide what should happen to the means. As physical power can only executed over physical things such an interpretation makes it necessary that the means are storage devices or computers.

[64] Footnote Working Paper, found on Mason, Electronic Signatures in Law, p. 150.
[65] Mason, Electronic Signatures in Law, p. 150.

### 3.1.4 Linked to the data that makes any change detectable

The hash value generated from the message is unique for every message because the operation from the message to the hash value is not reversible; it is not possible to generate from an arbitrary message a particular desired hash value and is computationally infeasible to find two messages with the same hash value.[66] Even the smallest changes are detectable.[67] This means that an advanced electronic signature detects subsequent changes of a message because the two hash values will not match.[68] The comparison between the two hash values fulfils this requirement.

If all these requirements are fulfilled, a public key infrastructure fulfils the requirements of the advanced electronic signature according to Art. 2 (2) ESD and Section 3 No. 2. ESA

### 3.1.5 Are there the same requirements for an advanced electronic signature?

There are some differences between the definition of an advanced electronic signature between the ESA and the ESD. One difference is that Art. 2 (3) ESD is using the term 'is linked to the data' while Section 3 No. 2 ESA is using the term 'linked to electronic data'. But actually there is no difference between those terms because Art. 2 (2) ESD defines an electronic signature as data in electronic form which is attached to (…) other electronic data (...). As 'the data' indicates a certain form of data the term points to the definition of in Art. 2 (2) ESD. One has to take into account that an electronic signature can only sign an electronic document and not a physical document.

More crucial is the following difference: The Directive says that the signature is 'linked to the data to which it relates'. The relation between the signature and the data is missing in the ESA. What is crucial is if this makes a difference in the meaning which does not comply with the Directive. The relation the Directive talks about means the relation between document and signature. As this relation is missing in the ESA there might occur the question if the ESA has not a wider definition of the advanced electronic signature than the Directive. But a signature

[66] Fegghi, Fegghi, Williams, Digital Certificates, p. 44.
[67] Fegghi, Fegghi, Williams, Digital Certificates, p. 46.
[68] Fegghi, Fegghi, Williams, Digital Certificates, p. 46.

which has no relation to the data of the signed document has no value because it has no function. The concept of a signature in a paper world is that it gives an indication that the document is produced by whoever signed it with all legal implications attributed to the signing by applicable law.[69] This presumption is based on the assumption that a handwritten signature is unique to everyone[70]. But that assumption does not work with an electronic signature,[71] because the electronic signature, which is a signed hash digest from the signed document does not have any function, actually does not work, without a document. As the Directive does not say what sort of relation should exist between the document and the electronic signature, it might be enough for the signature to be a mathematical result for which the document was one basic and important part. Because the whole signing operation would not work without document, there is a mathematical relation between the document and the signature. Another point is that the advanced electronic signature is thought to be the base for a qualified signature that fulfils the same functions as a handwritten signature. Therefore it should contain as well the implication about the origin of the data.

Therefore there is always an underlying mathematical relation between the electronic document and the electronic signature. As this relation indicates the hint about the relation which is given in the Directive the requirement might be a mere declaration instead of a mandatory requirement. As this relation is always there it is not necessary to write such an obvious thing into the implementation.

There is also a difference in the nature of sole control. The ESD requires for the sole control only the possibility of the signatory to have sole control over the means that creates an advanced electronic signature. The ESA is much stricter in this question because the sole control over the signature creation means seems to be mandatory. It is difficult to estimate what the phrase 'can maintain sole control' in the ESD means. It can mean the possibility to exercise alone physical power over signature creation means. For the storage devices with the signature-creation data means the possibility to exercise physical power that the access to them has to be secured, e.g. the access to the computerdata must be protected by a password or the smartcard should be

[69] Sinsi, Digital Signature Legislation in Europe, International Business Lawyer 2000, 487.
[70] Sinsi, Digital Signature Legislation in Europe, International Business Lawyer 2000, 487.
[71] Sinsi, Digital Signature Legislation in Europe, International Business Lawyer 2000, 487.

locked if it is not used. The other possible meaning is that the signatory just has to have the possibility to install such security means. But this last meaning would degrade the requirement sole control to a meaningless requirement because this opportunity to secure the access to a computer or other electronic data with a password is a normal technical possibility.

The ESA means that the signatory must have a physical control over the signature creation means. But such a physical control is not possible because it is not possible to watch always your computer or to hold a smart card always in your hands. Therefore the phrase 'maintain sole control' must be interpreted according to social habits. This means it must be reasonable for everyone that the signatory is exercising sole control. This is possible if he installs security measures such as the before mentioned access controls. Therefore the phrases 'maintain the sole control over signature creation means' and 'can maintain the sole control over signature creation means' have the same meaning: the possibility to exercise physical power over the access to the signature creation means.

Therefore Section 6 ESA complies with the definition of the Directive of an advanced electronic signature.

## 3.2 Qualified Certificate

Both laws require that the advanced electronic signature is based on a qualified certificate. Before explaining what a qualified certificate according to Art. 2 (10) ESD and Section 3 No. 2 ESA is, it is necessary to explain the use of a certificate in a public key infrastructure.

### 3.2.1 Certificate acc. to Art. 2 (9) ESD and Section 3 No. 9 ESA

A certificate is defined in Art. 2 (9) ESD and Section 3 No. 9 ESA as a link between signature verification data and the signatory which confirms the signatory's identity and is signed by the issuer of the certificate. Related to a public key infrastructure that means the pair of keys is linked to a natural or legal person or to an entity.[72] It answers the question how can someone know which two keys belong together and to whom? In a small community the keys might be passed to each other on a storage device, e.g. a USB stick. But digital signatures should ensure identification, authentication and data integrity in transactions between people who might have

[72] Feghhi, Feghhi, Williams, Digital Certificates, p. 61.

never met each other, e.g. via Internet. A physical exchange of storage devices is obviously not possible between them. The receiver of a message might identify the private key which belongs to the public key but how can he figure out who owns the private key? A certificate works as a sort of an identity card and binds a public key and a person or entity and maybe other attributes together.[73] With this binding everyone can find out who owns which pair of keys and can identify the sender of a message. This works only if it is possible to trust the certificate.[74] If everyone can design ones own certificate a certificate is considered to be not trustworthy. Therefore the system of certificates requires a certification authority which signs the certificate after issuing it. The signature of the certification authority itself is signed by another certification authority. So a hierarchical structure of certification authorities is built and one can decide at which level one trusts the certification authority.

[73] Dumortier, The Legal Aspects of Digital Signatures, Vol. II, p. 31.
[74] Feghhi, Feghhi, Williams, Digital Certificates, p. 64.

### 3.2.2 The requirements of Art. 2 (10) ESD/Section 4 ESA

A qualified certificate is not only an identification means as defined in Art. 2 (9) ESD and Section 4 ESA which links the signature-verification data to a person and that confirms the identity of that person. According to the definitions in Art. 2 (10) ESD and Section 4 S. 1 ESA, a qualified certificate has to meet the requirements laid down in Annex I ESD and in Section 4 ESA and is provided by a certification-service-provider that fulfils the requirements laid down in Annex II and in Section 10 to 15 ESA.

#### 3.2.2.1 Information Requirement according to Annex I ESD/Section 4 ESA

In Annex I ESD and Section 4 ESA information requirements have been laid down which a qualified certificate has to be able to contain. Some of the information has to be part of the certificate, some information has to be given the possibility to contain it.

Necessary information according to Annex I ESD are

- (a) an indication that the certificate is issued as a qualified certificate;
- (b) the identification of the certification-service-provider and the State in which it is established
- (c) the name of the signatory or a pseudonym, which shall be identified as such;
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
- (f) an indication of the beginning and end of the period of validity of the certificate;
- (g) the identity code of the certificate;
- (h) the advanced electronic signature of the certification-service-provider issuing it;

Information the certificate should be able to contain according to Annex I ESD are

- (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- (i) limitations on the scope of use of the certificate, if applicable; and
- (j) limits on the value of transactions for which the certificate can be used, if applicable.

Additionally Section 4 ESA allows that further details of the content of qualified certificates may be given in regulations prescribed by the King[75].

Annex I ESD and Section 4 ESA lay down a minimum standard for the information a certificate has to contain[76] as some information are obligatory. This should ensure a high level of trust and security regarding the correctness of the information contained because there are different types of certificates which contain different information and create therefore different levels of security and trustworthiness regarding the correctness of the information contained.[77] These information do not secure for a third party security regarding to the procedure followed during the registration process and issuing of the certificate because the signature of the certification service provider does not reveal his compliance with the rules of Annex II ESD. For some information the certificate is open to contain them but they are not obligatory information. Annex I ESD and Section 4 ESA are not bound directly to a specific technology existing today.[78] A common standard for certificates is the 509.x v3 standard.[79] According to RFC 5280 a certificate has different fields which contain certain information. Roughly the fields are divided into three groups: the tbsCertificatefield, the signatureAlgorithmfield and the subject field.[80] The three fields can be categorised as that one which contains information about entities, one which contains information to identify the CA and one which contains information to control the correctness of the information given about the subject and the CA.

One group contains only information about the certificate. Another group of fields contains information about the issuer. A third group of fields contains information about the subject. The information a X.509 certificate must or can contain makes it eligible to be a qualified certificate according to Art. 2 (10) ESD and Section 4 ESA because it can fulfil the requirements of Annex I. The different requirements of Annex I are fulfilled by the three groups of different fields.

---

[75] Unofficial translation by http://www.npt.no/ikbViewer/Content/1379/1379-electronic_signatures_act.pdf; visited 23.07.2009.
[76] Ot.prp.Nr. 82 (1999-2000), 8.4.1.
[77] Ot.prp.Nr. 82 (1999-2000), 8.4.1.
[78] Ot.prp.Nr. 82 (1999-2000), 3.3.
[79] Feghhi, Feghhi, Williams, Digital Certificates, p. 65; Schellekens 34.
[80] RFC 5280, ch. 4.1.1., p. 16 f.

#### 3.2.2.2 Is the definition of qualified certificate the same regarding the informational content?

There is a minor difference between the definition of a qualified certificate between the ESA and the ESD. The ESA lays down the requirement that the certificate expires one day that the ESD does not have. It looks as if the ESA imposes stricter rules on qualified certificates than the ESD. But as Annex I letter f) says that the certificate has to give information about the beginning and the end of the period of validity that implies that the certificate expires one day. Therefore the definition of a qualified certificate regarding the information the certificate has to contain comply with each other.

#### 3.2.2.3 Comply stricter information rules for qualified certificates with Art. 5 ESD?

In Section 4 S. 3 ESA the Norwegian King is able to adapt the information requirements a certificate should include and can impose stricter rules for qualified certificates. The Norwegian King is allowed to use a 'forskrift' which is defined in Section 2 Forvaltningsloven as a rule that applies to rights and duties for a not specified number or not specified group of people. As the requirements regarding the information a certificate should contain are minimum requirements, the King can in other regulations impose stricter rules about the information a qualified certificate should have. Therefore Section 4 S. 3 ESA complies with the ESD.

#### 3.2.2.4 Requirements the certification-service-provider has to fulfil

The second half of the definition of Art. 2 (10) ESD and Section 4 S. 1 ESA say that the qualified certificate which fulfils the requirements of Annex I has to be issued by a certification-service provider who fulfils the requirements of Annex II respective Sections 10 to 15 in the ESA. According to Art. 2 (11) ESD and Section 3 No. 10 ESA a certification-service-provider is an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. This means that certification-service-providers are not only those providers that issue a certificate but are services which are related to issuing and administration of certificates[81] which can be control of the identity of a signatory or the attribution of identifiable

[81] Ot.prp.Nr. 82 (1999-2000), 8.2.3.

names as well.[82] That can be for example the running of a certificate revocation list, a registry service for all certificates which are issued, archiving, time stamping, issuing of certificates or giving advice in relation to electronic signatures.[83] Giving advice in relation to electronic signatures can also mean giving advice regarding the acceptance of electronic signatures of an unknown certificate issuer.[84] All the mentioned services which are related to the issuing of a certificate can be given by a single service provider or by a group of service providers which can be business partners or subcontractors.[85]

The requirements which a certification-service-provider has to fulfil according to Annex II impose duties on the certification-service-provider. These duties can be grouped into three groups: information duties, information security duties and organisational duties concerning the organisation of the entity and the administration of the certificates. In detail the requirements of Annex II ESD can be grouped like this:

The information security duties are

- (f) Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
- (g) Take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature creation data, guarantee confidentiality during the process of generating such data;
- (i) Record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
- (j) Not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
- (l) Use trustworthy systems to store certificates in a verifiable form so that:
    - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, (...)

[82] Ot.prp.Nr. 82 (1999-2000), 8.2.1.
[83] Ot.prp.Nr. 82 (1999-2000), 8.2.1.
[84] Ot.prp.Nr. 82 (1999-2000), 8.2.1.
[85] Ot.prp.Nr. 82 (1999-2000), 8.2.1, 8.2.3.

These numbers contain the organisational duties concerning the organisation of the entity

- (a) Demonstrate the reliability necessary for providing certification services;
- (e) Employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
- (h) Maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance.
- (l) Use trustworthy systems to store certificates in a verifiable form so that:
    - only authorised persons can make entries and changes,
    - information can be checked for authenticity,
    - any technical changes compromising these security requirements are apparent to the operator.

The organisational duties concerning the administration of the certificates are defined in these points:

- (b) Ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- (c) Ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- (d) Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

The informational duty is laid down in

- (k) Before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any li-

mitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate.

If a certificate is issued by a certification-service-provider who fulfils all these duties laid down in Annex II ESD and in Section 10 to 15, a qualified certificate for the qualified signature has been created according to the definitions in Art. 2 (10) ESD and Section 4 S. 1 ESA.
The fulfilment of the requirements of Annex II ESD is according to Art. 3 (3) ESD at the moment monitored by each Member State independently. Therefore each Member State sets up its own regulation how to decide which certification-service provider fulfils the duties laid down in Annex II ESD. At the moment the Commission is carrying out a study which concentrates on a supervision model for certificate service providers which issue qualified certificates.[86]

[86] Commission action Plan, COM (2008) 798 final, p. 7.

#### 3.2.2.5 Requirements for certificate-service-providers comply with the requirements of Annex II

Within the requirements a certificate issuer has to fulfil the ESA has not implemented all requirements laid down in Annex II ESD.

##### 3.2.2.5.1 Letter l) Annex II ESD not implemented

The part of letter l) of the Annex II ESD according to which only qualified persons can make changes and entries into the certificate is missing. The government says that Annex II letter l) is not implemented into Norwegian Law because it is a requirement which is not needed in a public key infrastructure.[87] It is not possible in a public key infrastructure to change a certificate because a change of the content of a certificate means a withdrawal.[88] Such a change in the certificate makes it not valid according to RFC 5280 because one cannot see who has changed the content of the certificate. That causes doubts about the correctness of the content of the certificate and therefore causes doubts in the validity and trustworthiness of a certificate. The problem with this argumentation is that it shows how tight the law is fitted towards a PKI-structure whereas the Directive[89] and the ESA should be neutral towards a certain technology.[90] On the other hand there does not seem to be many alternatives to a PKI because it is the state-at-art technology. It was argued that requirement l) of Annex II ESD should be implemented into Norwegian law to take into consideration a further technological development.

##### 3.2.2.5.2 Letter e) Annex II ESD not implemented

What seems to be missing is letter e) of Annex II. Letter e) of Annex II ESD sets up requirements regarding the personnel a certificate issuer has to employ. This is an organisational matter. Section 10 S. 1 ESA deals with necessary law related, organisational, technological issues.[91] To be able to provide a secure and well functioning certification service this includes

[87] Ot.prp.Nr. 82 (1999-2000), 8.4.2.
[88] RFC 5280, 3.3 p. 12.
[89] Rec. 8 ESD.
[90] Ot.prp.Nr. 82 (1999-2000), 1.
[91] Ot.prp.Nr. 82 (1999-2000), 15.

dispositions related to personnel, operating and security.[92] This is indicated by 'manage their activities in a responsible manner' because the necessary dispositions to fulfil these requirements are to employ personnel who have the necessary expertise, knowledge, experience and qualification for the jobs.[93] This includes that the personnel are familiarised with electronic signatures technology as well as with proper security procedures.[94] Therefore letter e) Annex II ESD is implemented within the ESA.

[92] Ot.prp.Nr. 82 (1999-2000), 15.
[93] Ot.prp.Nr. 82 (1999-2000), 15.
[94] Ot.prp.Nr. 82 (1999-2000), 15.

## 3.3 Created by a secure-signature-creation device

The qualified signature has to be created by a secure-signature-creation device. A secure-signature-creation device is defined in Art. 2 (6) ESD and Section 8 ESA as a signature-creation device which meets the requirements laid down in Annex III respective Section 8 ESA.

### 3.3.1 Signature-creation-device

In Art. 2 (5) ESD and in Section 3 No. 6 ESA a signature-creation device is defined as configured software or hardware used to implement the signature-creation data which is defined in Art. 2 (4) ESD and Section 3 No. 5 ESA as unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. A signature-creation data can be the pair of keys or just the private key in a PKI-Infrastructure.[95] The signature-creation device is the medium the key in a PKI-Infrastructure is stored on.[96] This can be for example a smart card, which is often used.

### 3.3.2 Secure-signature creation device

To be a secure-signature-creation device the signature-creation device must fulfil the requirements of Annex III and Section 8 ESA, which are

- 1. Secure-signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
    - (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
    - (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
    - (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

[95] Brazell 5-055.
[96] Brazell 5-055.

- 2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

The Annex III/Section 8 requirements deal only with protection issues of the signature-creation data. Which technologies are in line with the requirements of Annex III/Section 8 is according to Art. 3 (4) ESD determined by an appropriate public or private body which is designated by the Member States. That body is a national body of a Member State which is established according to the criteria laid down in Commission Decision 2000/709/EC. Section 9 ESA rules the creation of that national body in Norway. Section 9 ESA says:

> "Approval as a secure signature creation device, cf. Section 8, is given by the body appointed by the King. The King may in regulations lay down more detailed provisions on that body and on requirements for secure signature creation devices.
>
> Approval from a corresponding body in another State which is a party to the EEA Agreement shall be considered equivalent to approval under the above paragraph.
>
> The requirements in Section 8 shall be considered to have been met when the hardware or software used conforms to the standards for electronic signature products which the European Commission lays down and which are published in the Official Journal of the European Communities."

The signature-creation device fulfils these requirements if it complies with the standards laid down by the EU-Commission or a national body according to Section 9 S. 3 ESA.[97] The King appointed a national body in Norway which certifies the security of IT-devices in accordance with Section 9 S. 1 ESA in Norway Nasjonal Sikkerhetsmyndighet (NSM).[98] NSM certifies according to the Common Criteria.[99] These requirements are part of a CWA which contains Protection Profiles[100] on which in a CEN Workshop it was agreed upon certain technical standards which fulfil EAL 4.[101] It should replace the expired reference number CWA 14167-1

[97] Ot.prp.Nr. 82 (1999-2000), 8.8.1.
[98] Section 13 Sikkerhetsloven.
[99] https://www.nsm.stat.no/Arbeidsomrader/Sertifisering-SERTIT/.
[100] CWA 14169:2004, p. 5, 30, 34.
[101] CWA 14169:2004, p. 5.

and CWA 14167-2 in 2003[102] of Commission decision in 2003 C(2003) 2439. These profiles do not cover the entire system environment in which secure signature-creation devices[103] operate because the requirements of Annex III should only ensure functionality of advanced electronic signatures.[104] The CWA states that there are different guidelines for the implementation of secure-signature-creation devices on different platforms.[105] They recognized three different types of secure-signature-creation devices.[106] Type one generates the signature-creation-data or the signature-verification-data.[107] This type can be a smartcard with a small microprocessor on it which is capable of generating the signature or verifying of the signatures.[108] Type two stores the signature-creation-data and creates the signature and needs a secure communication channel with a Type one device to gain the signature-creation-data.[109] This type can be a smart card which only stores information on its chip.[110] Type three can be described as a combination of type two and type one device because it generates the signature-creation-data and stores the signature-verification-data.[111] For this type is often a microprocessor smartcard used which chip is capable of calculating the algorithm for the signature-generation.[112] An approved secure-signature-creation device consists of a signature-creation device which means software or hardware used to create electronic signatures with the help of signature-creation data.

The existing technology is tested and approved by a national body established according to Art. 3 IV ESD. Technology that is approved by such a body fulfils the requirements of Annex III ESD/Section 8 ESA. So every system that is said to fulfil those requirements is a secure-signature creation device.

---

[103] CWA 14169:2004, p. 6, 11.
[104] Rec. 15 ESD.
[105] CWA 14169:2004, p. 6.
[106] CWA 14169:2004, p. 4.
[107] CWA 14169:2004, p. 31.
[108] http://www.smartcardbasics.com/cardtypes.html; visited 21.07.2009.
[109] CWA 14169:2004, p. 95.
[110] http://www.smartcardbasics.com/cardtypes.html; visited 21.07.2009.
[111] CWA 14169:2004, p. 169.
[112] http://www.smartcardbasics.com/cardtypes.html; visited 21.07.2009.

### 3.3.3 Does an approved secure signature-creation device fulfil the requirements of Annex III?

The requirements Section 8 ESA lays down for a secure signature-creation device comply with the definition of a signature-creation device and the requirements of Annex III ESD. The only difference seems to be that the secure signature-creation device has to be approved according to Norwegian law but the Directive has laid down that requirement not in the definition of a secure signature-creation device but in Art. 3 (4) ESD. Art. 3 (4) ESD says that the conformity of a signature-creation device with the requirements of Annex III ESD should be approved by an appropriate body the Member State designates according to the procedure laid down in Art. 9 ESD. Therefore the definition of an approved secure signature-creation device is in line with the definition of the Directive.

### 3.3.4 Are the protection profiles of the common criteria page accepted in Norway?

The Norwegian NSM certifies signature-creation devices according to the rules of Common Criteria.[113] The rules for secure signature-creation devices have been laid down in Protection Profiles which can be found on the HP of the Common Criteria.[114] Protection Profiles are accepted for secure-signature creation devices in Norway because these are international standards which are laid down as well in the CWA 14169.

## 3.4 Are there the same requirements for a qualified signature?

Qualified signatures in the Directive are according to Art. 5 S. 1 advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device. That is the same definition as in Section 3 3. ESA which says that a qualified signature is an advanced electronic signature which is based on a qualified certificate and created by an approved secure-signature creation device. This sounds as if the requirements for a qualified signature are congruent but there might be differences in the details. Therefore I will have a closer look at the differences in the details of the definitions.

[113] Ot.prp.Nr. 82 (1999-2000), 8.8.1.
[114] Ot.prp.Nr. 82 (1999-2000), 8.8.1.

## 4 Legal consequences for a qualified signature

In both laws the qualified signature is granted the same legal recognition like handwritten signatures.

### 4.1 Art. 5 I ESD

Art. 5 I ESD gives equivalence to a qualified signature in that way that it takes the handwritten signature as a reference point for what an electronic signature should be.[115]

#### 4.1.1 Satisfy the legal requirements of a signature – Art. 5 ESD

The term ‘legal requirement' in Art. 5 ESD means every requirement which is set up for a signature in a legal rule. This can be for example the requirement ‘handwritten’ for the signature in a will in Section 2247 BGB.

#### 4.1.2 Qualified signature in relation to electronic data equals handwritten signature in relation to paper-based data – Art. 5 ESD

A paper-based document, combined with a handwritten signature, is assumed to be authentic in a very secure way.[116] Although that is not true because it is very easy to falsify a handwritten signature, the handwritten signature is a well-known and accepted authentication means.[117] The handwritten signature has gained a symbolic character and represents today the means of authentication which provides a high level of legal certainty.[118]

An electronic document needs authentication in the same way as a paper-based document. A technology is presumed to fulfil the same functions as a handwritten signature if it fulfils these 8 authentication characteristics: data origin authentication, non-repudiation, integrity, link between

[115] Dumortier, The legal market and aspects of electronic signatures, p. 50
[116] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 56.
[117] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 57.
[118] Dumortier, The Legal aspects of Digital signatures, Vol. II, p. 57.

the authentication tool and the content, difficult to forge, easy to verify, verifiable as long as the legal act is of legal importance and allows entity authentication.[119] The technological description the Directive points at is a digital signature that is based on asymmetrical encryption. That technology helps to authenticate the origin of the data, shows the non-repudiation of the document and guarantees the integrity of the document. It links the authentication tool with the content because the data to calculate the signature is partly originating from the signed document. It is difficult to forge because it uses some complex mathematical calculations while it is easy to verify with the public key of the sender as long as the legal act is of legal importance because the certificate can be remain retrievable as long as the digital signature is needed.[120]

[119] Dumortier, The Legal aspects of Digital signatures,Vol. II, p. 54ff.
[120] Dumortier, The Legal aspects of Digital signatures,Vol. II, p. 77.

### 4.1.3 Legal effect and admissibility as evidence

The question arises if a qualified signature is admissible as evidence because there is no extra regulation for that in the civil procedure law or in the ESA. The principle of free giving of evidence allows parties to give as evidence what they think is necessary. Therefore qualified signatures are admissible as evidence under this principle; this means in civil procedure law a qualified signature is admissible as evidence.

## 4.2 Section 6 S. 1 ESA

The reference point for a qualified signature is also a handwritten signature.

### 4.2.1 Contains signatures – Every rule concerning legal effects of a signature

Section 6 S. 1 ESA only concerns rules that requires a signature as formal requirements. The signature has different functions. The functions a signature can have are different and the degree of importance can be varying.[121] A signature can have evidential functions, cautionary functions, protective functions, channelling functions and record keeping functions. Within the evidential functions primary and secondary evidential functions are distinguished.[122] The primary purpose of a signature serves to provide admissible and reliable evidence to the following 3 elements: the signatory approves and adopts the contents of the document and thereby agrees that the content of the document is binding upon them and has legal effect.[123] The signature reminds the signatory about the significance of the act and the need to act within the provisions of the document.[124] As secondary evidential functions a signature is capable of providing identification and proof of the authentication of a person's identity, the identity of a particular characteristic, attribute, status of a person, e.g. the status as a company director.[125] The cautionary function means that the signatory should take care before committing themselves to the contents of the

[121] Mason, Electronic Signatures in Law, p. 20.
[122] Mason, Electronic Signatures in Law, p. 20.
[123] Mason, Electronic Signatures in Law, p. 20.
[124] Mason, Electronic Signatures in Law, p. 20.
[125] Mason, Electronic Signatures in Law, p. 20.

document.[126] The protective function is related to the cautionary function. This function gives the receiving party some security that the other party affirms the content of the document and they have given their full attention to the content of the document.[127] The channelling function means that the signature helps to clarify the point at which a person recognises the act has become legally significant.[128] The record keeping function means that a document which is manifested in a physical format serves as a durable record of the terms of an agreement.[129] This shows that different laws appoint to handwritten signatures more functions than those information security purposes appoints to them.

[126] Mason, Electronic Signatures in Law, p. 21.
[127] Mason, Electronic Signatures in Law, p. 21.
[128] Mason, Electronic Signatures in Law, p. 21.
[129] Mason, Electronic Signatures in Law, p. 21.

### 4.2.2 In order to obtain a specific legal effect

The use of a signature should have a legal consequence. For example in Germany a will shall not be valid until it is signed says Section 2247 I BGB if it is not testified by a notary.[130] In general a signature can be used for authentication and identification.[131] But in connection of the requirement of a written form it can also function as a warning and information[132] because if someone has to put his signature under a document this warns him that he is doing something which binds him. These functions one usually finds in the law. If one takes the example of Section 2247 BGB the signature has got the function to identify and authenticate the person who wrote that will.

### 4.2.3 Provision may be implemented electronically

With the provision is meant every rule which binds a legal effect to a signature. These provisions should be capable of being used in an electronic environment. That means that there must be a legal possibility to communicate electronically within the actual area of law, otherwise Section 6 S. 1 is not applicable.[133] This border is implemented because there are rules which cannot be implemented electronically.[134] The example with Section 2247 BGB is not a usable example here because Section 2247 BGB requires a handwritten will with a handwritten signature which is not possible in an electronic environment as electronic wills seem in general not to be accepted.[135] Without this border Section 6 S. 1 ESA will apply wider as it should be and is wished.[136] In relation to electronic signatures an electronic environment means a means of electronic communications, e.g. via e-mail, via Instant Messenger Services or via other electronic communications means.

---

[130] See section 2231 BGB on http://bundesrecht.juris.de/englisch_bgb/englisch_bgb.html#BGBengl_000P2247; visited 24.07.2009.
[131] Mason, Electronic Signatures in Law, p. 2.
[132] Ot.prp.Nr. 82 (1999-2000), 8.10.1.
[133] TOBYF-2004-598.
[134] Annex to Innst.O. nr. 41. 41 (2000-2001), § 6.
[135] Annex to Innst.O. nr. 41. 41 (2000-2001), § 6.
[136] Annex to Innst.O. nr. 41. 41 (2000-2001), § 6.

### 4.2.4 Consequence for the qualified signature

If a qualified signature fulfils all the above mentioned requirements the requirements set up for the signature apply for the qualified signature as well. Section 6 S. 1 ESA gives therefore the same legal recognition to qualified signatures like handwritten signatures[137] because they are given the same legal consequence as a handwritten signature if the rule concerning the requirement of a signature can be implemented electronically.

## 5 Art. 5 II ESD/ Section 6 S. 2 ESA

Both second parts of the two laws set up rules for the legal recognition of an electronic signature as defined in Art. 2 (a) ESD/ Section 3 1. ESA. Both laws define the 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.

### 5.1 Art. 5 II ESD

Art. 5 II ESD is a non-discrimination rule for electronic-signatures. An electronic signature is according to the definition in Art. 2 (1) ESD data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. This definition gives the term electronic signature a wide meaning because it means every data which identifies and authenticates.[138] That can be as simple as signing a message with a person's name[139] or a picture of a handwritten signature.[140] Some disagree with the concept that a typed name under an E-Mail or a scanned handwritten-signature can serve as a signature because an electronic document differs in its nature from a paper document.[141] To serve the functions of the

[137] Ot.prp.Nr. 82 (1999-2000), 8.10.1.
[138] EU-Commission Report, COM 2006/120 final, p. 4.
[139] EU-Commission Report, COM 2006/120 final, p. 4;.
[140] Brazell 5-042.
[141] Sjöberg/Nordén, Managing Electronic Signatures, 83.

above mentioned authentication definition electronic documents must have a special relation with each other because it is necessary that they are connected with each other electronically. This means that a series of electronic impulses have to be connected with another series of electronic impulses in a way that changes can be detected. A name tag or a scanned handwritten-signature do not provide such an electronic connection. This premise speaks against those who consider a typed name under an E-Mail or a scanned handwritten-signature as an electronic signature. But it is socially more common to assign electronic forms the same functions as paper forms. A lot of people who use electronic forms tend to give them a social meaning to that what they can observe about the electronic impulses. For example, people take the displayed form of an electronic document as the document and 'translate' what they see into known social functions. Therefore some say that a typed name under an E-Mail or a scanned handwritten signature are able to fulfil the concept of an electronic signature because they see a similar format to the paper format. I think that a name tag under an E-mail can be a signature because ESD and ESA have got different levels of signatures which are attached to different sorts of technologies on different sophisticated levels. The basic form is not attached to specific technology unlike the two more sophisticated forms of electronic signatures in both laws. The point that illustrates this motivation is that the social understanding gives the handwritten signature the concept it has today. The law should leave room to develop a social understanding of electronic forms. This is only possible if there is no further technological premise connected to the basic form of an electronic signature.

Art. 5 II ESD gives four reasons on which an electronic signature cannot be denied legal effectiveness and admissibility as evidence in legal proceedings. The reasons are

- In electronic form
- Not based upon a qualified certificate
- Not based upon a qualified certificate issued by an accredited certification-service-provider
- Not created by a secure signature creation device.

Basically Art. 5 II ESD means that an electronic signature does not have to be a qualified signature to gain legal recognition.[142]

The question occurs if the non-discrimination rule only applies to electronic signatures as defined in Art. 2 (1) ESD and not to advanced electronic signatures as defined in Art. 2 (2) ESD. This would lead to the result that it would be compliant with Art. 5 II ESD to discriminate an advanced electronic signature. One can argue that there are two different definitions in Art. 2 ESD which means that both forms of electronic signatures are two different things. If one takes the technical background of the different electronic signature one can definitely say that both definitions mean different things. But as the Directive takes a technically neutral approach[143] towards electronic signatures different techniques which form the background of the definitions are not relevant for the question. Art. 5 II ESD sounds like a basic rule for legal recognition of electronic signatures.[144] The definition of Art. 5 II ESD is wide and contains the definition of Art. 2 (2) ESD because Art. 2(2) ESD only describes a certain technology which is used to identify and authenticate a person. Therefore the non-discrimination rule gives legal recognition to all sorts of electronic signatures. The simplest methods such as a name, initials, a pseudonym, scanned handwritten signature under an electronic document[145] to provide an electronic signature fall under the definition of Art. 2 (1) ESD.[146] They provide a very low level of assurance to the identity and the authenticity of an individual.[147]

## 5.2 Section 6 ESA

Section 6 S. 2 ESA says that an electronic signature which is not a qualified signature can fulfil the requirements for a rule which lays down a signature as a requirement. This means that an electronic signature which is not a qualified signature can be equivalent to a handwritten signature[148] but this is not a necessity. The question if an electronic signature fulfils the formal requirements to gain equivalence to a handwritten signature depends on the type of electronic

---

[142] Encyclopedia of information technology law, 3.249/3.
[143] Recital 8 ESD.
[144] EU-Commission Report, COM 2006/120 final, p. 4.
[145] Brazell, 3-004 – 3-009.
[146] Brazell, 3-010.
[147] Brazell, 3-010.
[148] Ot.prp.Nr. 82 (1999-2000), 8.10.3.

signature.[149] It may be possible that an electronic signature must not be equivalent to a handwritten signature but is eligible as evidence because it proves beyond doubt a certain fact, e.g. an electronic timestamp proves when a document has arrived and can therefore be used as a piece of evidence if a deadline is held or not. Section 6 S. 2 ESA gives the respective electronic signature that content as piece of evidence which serves the function of the electronic signature best. Therefore the approach is highly flexible.

[149] Ot.prp.Nr. 82 (1999-2000), 8.10.3.

## 5.3 Does the non-discrimination rule results from normal Norwegian law?

If one compares Art. 5 II ESD and Section 6 ESA, it is obvious that the non-discrimination rule of Art. 5 II ESD is missing. The question is if that is a breach of the EEA-Agreement. There is a breach of the EEA-Agreement if the non-discrimination rule has to be transferred into Norwegian law. As Art 5 ESD is a central part of the signature it is very important to implement the non-discrimination rule of Art. 5 II ESD into Norwegian law.[150] It belongs to the mandatory part of the Directive.[151] Therefore it must be implemented into Norwegian Law. But it is not necessary to implement the non-discrimination rule of Art. 5 II ESD, if the non-discrimination rule is already part of Norwegian law. Then an incorrect implementation of the ESD does not exist and the EEA-Agreement is not breached. In its reasoning the Norwegian government argued that the non-discrimination rule is already part of the Norwegian law.[152] The principle of free giving of evidence and the free consideration of evidence means that an electronic signature is admissible as evidence before court, no matter if it is a qualified signature or not.[153] The non-discrimination rule is regulating the legal effectiveness and the admissibility as piece of evidence of an electronic signature.

### 5.3.1 Legal effectiveness of an electronic signature

The legal effectiveness of an electronic signature is implemented in the second sentence of Section 6 ESA because it says that an electronic signature can meet the same requirements as a qualified signature and has therefore the same legal recognition. The legal effectiveness of an electronic signature means any legal consequence an electronic signature is given. This can be the possibility to conclude legal valid agreements between private parties, the acceptance of electronically signed documents between private parties or in all kinds of administrative procedures or the evidence electronic signatures can give in court litigation.[154] But Section 6 S. 2 ESA concerns just the highest level of the legal recognition an electronic signature can get, not

[150] Innst.O. nr. 41. 41 (2000-2001), 3.
[151] Ot.prp.Nr. 82 (1999-2000), 2.
[152] Ot.prp.Nr. 82 (1999-2000), 8.10.2.
[153] Ot.prp.Nr. 82 (1999-2000), 8.10.2.
[154] Dumortier, The Legal aspects of Digital signatures,Vol. VI, p. 23.

the bottom line of legal effectiveness.[155] It gives the judge a wide guideline what function an electronic signature can serve. The second sentence of Section 6 ESA says that an electronic signature can have the same effect as a handwritten signature and limits the legal recognition of an electronic signature to this point. This is the same with Art. 5 ESD rules because Art. 5 II ESD does not give a presumption what functions an electronic signature can serve. Therefore an electronic signature can have the same legal recognition as a handwritten signature. But this probable equivalence of an electronic signature does not necessarily mean that an electronic signature cannot be discriminated because it is electronic, not based upon a qualified certificate, not based upon a qualified certificate by an accredited certification-service-provider or not created by a secure signature-creation-device. This minimal legal recognition seems to be missing for the legal effectiveness in Section 6 ESA.

The principle of free consideration of evidence does not cover all parts of the legal effectiveness of an electronic signature. There are other areas except the consideration as evidence before court where the legal effectiveness of an electronic signature can be important. For example can an electronic signature verify the authenticity in electronic communication between a citizen and a township. If the township does not recognize an electronic signature as valid because it is electronic or because it does not fulfil the requirements of a qualified signature although a handwritten signature would be not necessary within the communication process the electronic signature would be discriminated. Legal effectiveness is as well granted if a legislator gives a certain legal consequence to an electronic signature.

[155] Annex to Innst.O. nr. 41. 41 (2000-2001), § 6.

#### 5.3.1.1 Legal effectiveness found in the principle of free consideration of evidence

Section 21-2 (1) Tvisteloven says that a judge can consider freely the given evidence. The consideration is based according to Section 21-2 (2) Tvisteloven on that what is found as factual circumstances. The principle of free consideration includes that the judge's consideration is neither bound by how much weight certain evidence should attached to[156] nor bound to the party's argumentation about a question of evidence,[157] which is ruled explicitly in Section 11-2 S. 3 Tvisteloven. The question is if the principle of free consideration of evidence gives the judge the possibility to reject an electronic signature because of the reasons which are forbidden according to the non-discrimination rule of Art. 5 ESD. The free consideration of evidence has consequences for what the electronic signature proves. In the case of an electronic signature this means more or less if the electronic signature proofs the integrity of the electronic communication and the authenticity of the sender of the document.[158] What this means in a single case is dependant of different considerations made by the circumstances how the electronic signature is used. This means according to the ESD it is correct to consider the authentication of the non-qualified signature on a lower level if the signature is not qualified according to Art. 5 I ESD/ Section 6 S. 1 ESA because the authentication a qualified signature gives is equalised with a handwritten signature. Both rules allow the possibility that a judge can deny a legal effect of an electronic signature. The non-discrimination rule expects from a judge that a denial of an electronic signature is based on an affirmative finding, e.g. lack of technology reliability or accountability. [159] But the consideration of evidence should be complete, thorough and efficient.[160] A thorough consideration of an electronic signature as evidence might not be a denial of a legal effect of an electronic signature just because it is electronic or does not fulfil the requirements of a qualified certificate. The principle of free consideration of evidence makes it unlikely that a judge denies the legal effect out of the forbidden reasons of Art. 5 II ESD because these reasons are build on a general argument. Such an argument Art. 5 II ESD wants to hinder

[156] Schei, § 21-2 Tvisteloven, Nr. 1, § 11-2 Tvisteloven, Nr. 10.
[157] Schei, § 21-2 Tvisteloven, Nr. 1, § 11-2 Tvisteloven, Nr. 10.
[158] Fischer-Dieskau, Gitter, Paul, Steidle, MMR 2002, 709.
[159] Dumortier, The Legal and Market Aspects of Electronic signatures, p. 51.
[160] Nou 2001, p. 458.

because a denial of legal effects should be based on an evaluation and should be sufficiently reasoned.[161] But an unlikelihood is not the certainty a non-discrimination rule would give. The possibility is still there that a judge considers the denial of legal effect of an electronic signature because it is electronic or it does not fulfil the requirements of a qualified signature to be thorough, efficient and complete in a case.

The principle of free considering of evidence is not written down in the Straffeprosessloven but it is considered to be such a general rule in Norwegian evidence law that it can be erased.[162] There are the same rules used as in the Tvisteloven. Therefore the conclusion for electronic signatures in a criminal law case before court is the same: The judge might consider an argument as sufficient consideration that is forbidden according to Art. 5 II ESD. This result might be improbable but because the judge decides if he considers a general argumentation as sufficient enough to deny electronic signatures legal recognition, such a result is possible.

[161] Dumortier, The Legal and Market Aspects of Electronic signatures, p. 51.
[162] Andenæs, Norsk Straffeprosess, p. 183.

#### 5.3.1.2 Legal effectiveness found in other areas

Regarding the legal effect an electronic signature has outside of courts the non-discrimination rule of Art. 5 II ESD has to be taken into account as well.[163] This means that a legislator or another state institution can deny the legal effect of an electronic signature as defined in Art. 2 a) ESD/ Section 3 1. ESA only sufficiently reasoned and based on an evaluation[164]. As Section 6 S. 2 ESA applies to legal effects of electronic signatures outside of courts as well this means that such an institution can give an electronic signature the same legal effect as a handwritten signature. However as the principle of free consideration of evidence is only binding courts Section 6 S. 2 ESA might allow a general discrimination of an electronic signature because it is not a qualified signature or because of its electronic form. But if the non-discrimination rule can be implemented in another way such discrimination is hindered. If in a law the use of an electronic form with an electronic signature is allowed it is impossible to reject an electronic signature because it is not fulfilling the requirements of Art. 5 I ESD or electronic. The Norwegian government has done this: for example it uses a general understanding for document in Section 3 Offentlighetsloven and Section 2 f) Forvaltningsloven which is not bound to paper and it expanded the meaning of written in that way that written implies also an electronic message. In this point Section 6 S. 2 ESA does comply with the Art. 5 2 ESD.

But one has to take into account that a legislator can consider in a legislative act that an electronic signature is denied a legal effect because of its electronic format or its non-qualified nature[165]. This effect is reduced by general form rules such as Section 3 Offentlighetsloven and Section 2 f) Forvaltningsloven because the equivalence between written and electronic form these provisions give complicates such rules. But these rules does not hinder exemptions from the mentioned rules. Therefore Section 6 S. 2 ESA does not comply with Art. 5 2 ESD.

---

[163] Dumortier, The Legal and Market Aspects of Electronic Signatures, p. 51.
[164] Dumortier, The Legal and Market Aspects of Electronic Signatures, p. 51.
[165] Dumortier, The Legal and Market Aspects of Electronic Signatures, p. 51.

### 5.3.2 Admissibility as evidence

The question is if the non-compliance of the non-discrimination rule into Norwegian law opens the door for judges to reject an electronic signature as evidence which is not a qualified signature because it is electronic, not based upon a qualified certificate, not based upon a qualified certificate by an accredited certification-service-provider or not created by a secure signature-creation device. As it would be too far fetched within this thesis to give a detailed overview over the whole Norwegian law concerning evidence before different sorts of courts only the general rules concerning the admissibility of evidence of the Tvisteloven, which is the civil procedures law and of the Straffeprosessloven, which is the criminal procedures law will be mentioned. This will be sufficient as an overview because there seems to be an incorrect implementation through the missing non-discrimination rule.

If a judge considers evidence he has to accept it as evidence first. Therefore he cannot reject an electronic signature as admissible because it is electronic or does not fulfil the technical requirements of a qualified signature. He can though reject the argument of the party what the electronic signature should prove.

Section 21-3 Tvisteloven regulates what is admissible as evidence. In Section 21-3 (1) Tvisteloven the parties have the right to give evidence as they wish except for the exemptions made in the Tvisteloven and the exemptions that result from §§ 21-7, 21-8 and chapter 22 Tvisteloven. The principles of free consideration of evidence and free giving of evidence are linked together.[166] But there is only an incorrect implementation of the ESD if the principle of free giving of evidence opens the possibility for a judge to reject an electronic signature as evidence because of the reasons laid down in Art. 5 II ESD. If the parties have according to Section 21-3 Tvisteloven the possibility to admit as evidence what they wish, there seems to be no possibility of a rejection of the judge due to the 'forbidden' reasons of Art. 5 II ESD. The problem is that the law as such makes exemptions from this rule and these exemptions are extensive.[167]

---

[166] Schei, § 21-2 Tvisteloven, Nr. 2; § 21 – 3 Tvisteloven, Nr. 2.
[167] Schei, § 21 – 3 Tvisteloven, Nr. 2.

Section 21-7, Section 21-8 and Section 9-16 (II) Tvisteloven deal with general exemption for the admissibility of evidence due to process economical reasons. These exemptions are concerned with denial of evidence which is not necessary for the case, which has just a small meaning for the case, which is not adequate for the case or which is brought forward to late. A denial of admissibility founded on these reasons is not related to the reasons of Art. 5 II ESD. Chapter 22 Tvisteloven contains prohibitions of taking evidence due to disclosed information in Sections 22-1 to 22-8 Tvisteloven and rights to refuse giving evidence in Sections 22-8 to 22-12 Tvisteloven. These limits do not fall under the non-discrimination rule of Art. 5 II ESD either.

Section 21-12 Tvisteloven gives in its second subsection denial for written documents from experts under certain conditions. These conditions have nothing to do with the quality of an electronic signature or its electronic nature, therefore this rule complies with the non-discrimination rule.

The Straffeprosessloven does not contain a special rule for the free giving of evidence. The principle of free giving of evidence is part of the Straffeprosessloven as well because there are only a few rules that lead to an inadmissibility of evidence.[168] The starting point in Norwegian criminal procedure law is that the parties in a criminal law 'investigation' can give that evidence they think is connected to the case.[169] To evaluate which rules may prohibit this principle there must be distinguished between very general prohibition rules and rules which are made for special material of evidence.

Again the Straffeprosessloven states in Section 292 S. 2 a - c Straffeprosessloven that evidence which has no relevance for the case. The regulation includes a general and a specific relevance for the fact that should be proofed. The reason of the prohibition of evidence is here not based on the electronic nature or the missing fulfilment of the requirements of a qualified certificate. Therefore this prohibition does comply with Art. 5 II ESD. The same result can be found for the rules in Sections 293 and 295 Straffeprosessloven because these rules prohibit the giving of evidence because they are based on process economic reasons and are not able to interfere with the non-discrimination rule of Art. 5 II ESD.

---

[168] Rt. 1990-1008; Andenæs, Norsk Straffprosess, p. 183.
[169] Rt. 1990-1008.

Section 92 and 136 Straffeprosessloven comply with Art. 5 II ESD because they deal with methods to get a statement from a witness or the defendant.

The same is valid for Sections 117 to 120, 134, 301 Straffeprosessloven because they deal with statements of witnesses before court or during the investigation. Usually are there no electronic signatures used.

The rule that illegal obtained evidence[170] complies with Art. 5 II ESD because the reason for the rejection of evidence in this Section is the illegal way the evidence was obtained.

Section 302 Straffeprosessloven applies to written documents. Usually electronic documents are not understood as written documents. Therefore Section 302 Straffeprosessloven does not apply to electronic signatures related to electronic documents. To fulfil the principle of speech acc. to Section 278 Straffeprosessloven the electronic document and electronic signature must be presented in some way before court.

There are certain prohibitions for certain evidence. To see if this prohibition applies to an electronic signature, it must be evaluated what sort of evidence an electronic signature is. In the Straffeprosessloven there is evidence called gransking, which is an examination of evidence. This means every real thing as evidence, for example tissues, documents or pictures.[171] As these regulations apply to everything, they could apply to electronic documents and especially to electronic signatures. The problem is what 'real' means. Does it only mean concrete things, such as paper, tissues or goes the meaning of 'real' further because usually there is a distinction between a 'real' world and a 'virtual', often meant electronic, world. Because an electronic signature is something not concrete, not touchable, one could say it is not real evidence. The problem which occurs now is what evidence is an electronic signature then if it does not fall under gransking? That result would lead to a discrimination of electronic signatures. Therefore electronic signatures and electronic documents would be discriminated as evidence because they are electronic. This interpretation would not comply with Art. 5 II ESD. Another point to think about is if a document, written or electronic, is given as evidence, usually the content is

[170] For further description of this principle in Norwegian law: see Rt. 1992 698 (702-706); Andenæs, p. 268 ff.; Anders Bratholm, TFR-1959-109.

[171] Hustad, Straffeprosessloven, Chapter 12, Note 923, found on: http://abo.rettsdata.no/propub/template.htm?s_terms=""&view=browse&doc_action=setDoc&doc_keytype=tocid&bid=toc&doc_key=0519340303#top

important. Without doubt written documents fall under this rule. In an electronic document the content is as important as it is in a written document. Therefore electronic documents and electronic signatures fall under the special rules of gransking. That means that there is no discrimination of an electronic signature as admissible evidence.

## 6 Why does the Directive apply to Norway?

The EEA Agreement says in Art. 7 (b) EEA-Agreement that acts which are referred to or contained in the Annexes of the Agreement or in decisions of the EEA Joint Committee should be implemented into the internal legal order of a contractor of the Agreement if the act is corresponding to an EEC Directive in a form chosen by the authorities of the Contracting Parties. Norway is a Member of the EEA. Annex XI No. 5l EEA Agreement contains the ESD. The EEA-Agreement was implemented into Norwegian Law through the EØS-Loven in 1992. Section 1 EØS-Loven requires that the main part of the EEA-Agreement is part of the Norwegian Law. Therefore the ESD has to be implemented according to Art. 7 b) EEA Agreement into Norwegian Law. As there is a core part missing in the ESA, the non-discrimination rule of Art. 5 II ESD, the question arises how a directive applies in an EEA-Member if it is not fully implemented.

### 6.1 Direct application of the Directive based on legislation/contract

Section 2 EØS-Loven sets up a rule of precedence if the EEA-Law and the national are opposite to each other.[172] This rule does not apply with the Directive because national law does not clash with EEA-Law but EEA-Law is not implemented correctly into Norwegian law.

The EEA-Contract does not contain a rule what consequences are following if EEA-Law is not or not correctly implemented.[173]

### 6.2 Direct application of the Directive based on EEA-Law

The two leading cases which help to discuss this problem with regard to Norwegian Law are the Finanger Cases of the Norwegian Supreme Court.[174] According to these two decisions the question is not answered easily and clearly. The main problem is, if the EEA-Law has horizontal

[172] Rt. 2000, 1826.
[173] Efta Court, Case E-9/97, 46; Rt. 2005 1690, (45).
[174] Harbo, Nordic Journal of International Law 78 (2009) 201 (205).

effect in the Norwegian Law or not if EEA-Law was not implemented correctly. The Finanger I decision was not unanimous. The Norwegian Supreme Court denied a direct application of a Directive because the horizontal effect infringes the intergovernmental character of the EEA-agreement.[175] The main reasoning is that Art. 7 EEA-Agreement states that a Directive has to be implemented into Norwegian Law by Norwegian authorities.[176] This means that a Directive has no horizontal effect in Norwegian law in general.[177] A dissenting opinion came to the conclusion that the Directives have horizontal effect, because there is no difference how far the Directives reach in EU and EEA-Law.[178] The incorrect implementation of the EEA-Law can be corrected by the interpretation of the court because the legislator wanted to fulfil his obligation of the EEA-contract when he implemented the Directive.[179] But the judges have to show some respect towards the intentions of the legislator when he implemented a Directive in the way he did.[180]

The Directives can only be an aspect in the interpretation of a Norwegian Law based on a Directive because the EEA-agreement and the 'presumsjonsprinsippet' require an interpretation that complies with the Directive.[181] A breach of international public law must be hindered.[182] This means that a court might ignore national law.[183] This interpretation is necessary as EEA members have the duty to show loyalty towards the EEA-Agreement and its rules.[184] This loyalty duty is accompanied by the principle of the homogeneity of law within the EU.[185] With this reasoning the first argumentation cannot deny the direct effect of Directives in Norway.[186] But the general difference between the EU and the EEA is that it is an agreement between the EU and the EFTA States. The EFTA was thought to be an opposite model about economic cooperation between European States.[187] There are no supranational organs because the EFTA is

[175] Harbo, Nordic Journal of International Law 78 (2009) 201 (205).
[176] Rt. 2000, 1826.
[177] Rt. 2000, 1826.
[178] Rt. 2000, 1837.
[179] Rt. 2000, 1836.
[180] Rt. 2000, 1831.
[181] Rt. 2000, 1826.
[182] Rt. 2000, 1839.
[183] Rt. 2000, 1840.
[184] Rt. 2000, 1827.
[185] Rt. 2000, 1827.
[186] Rt. 2000, 1840.
[187] Schymik, Norwegens Sonderweg nach Europa, p.9.

thought to be an intergovernmental cooperation[188] not a supranational bundle of states like the EU. This difference explains according to the reasoning of Finanger I why there is no horizontal effect of a Directive if it is not implemented correctly.[189] The judgement says that a horizontal effect of a Directive in Norway would go beyond the scope of the interpretation according to Directives in EU-Law.[190] Therefore it is the task of the legislator to react if a Directive is not implemented correctly.[191] There is no reason for a court to use the rule of direct conform interpretation or the 'presumsjonsprinsippet' to interpret away a clear rule in national law[192] although the judges should use all methods of interpretation to avoid a breach of international public law.[193] The EEA-Agreement did not take over the principle of precedence as it is found in EU-Law.[194] Another result in this question would mean a legal uncertainty for ordinary people because they cannot rely on the national law.[195] This shows that foreseeability and conversion has to be considered in this question as well.[196] The predictability is quite complex and put together from different legal sources because the EEA is according to the Sveinsbjørnsdottir-case a distinct legal order of its own.[197] The EU-Directives are partly interpreted from other legal sources than that ones used in Norway.[198] In Norway these interpretations are binding[199] which can be found in the decisions of the ECJ. Therefore the EEA-Members had to take over the rule that if a national rule is in conflict with implemented EEA-Law or other laws it has to be implemented a regulation in the law that the EEA- Law is prioritised.[200]

## 6.3 State Liability based on the EEA-Agreement

The Norwegian Supreme Court has given the state liability for the incorrect implementation of a Directive in the Finanger II Case. This decision was again not unanimous. In the Finanger Case

---

[188] Harbo, Nordic Journal of International Law 78 (2009) 201 (203).
[189] Rt. 2000, 1831.
[190] Rt. 2000, 1831.
[191] Harbo, Nordic Journal of International Law 78 (2009) 201 (205).
[192] Rt. 2000, 1831.
[193] Rt. 2000, 1830.
[194] Rt. 2000, 1831.
[195] Rt. 2000, 1832.
[196] Rt. 2000, 1840.
[197] Rt. 2000, 1840; Efta Court, E-9/97, 59.
[198] Rt. 2000, 1840.
[199] Rt. 2000, 1840.
[200] Rt. 2000, 1828.

the Norwegian Supreme Court followed mainly the argumentation of the EFTA-Court.[201] In the Sveinsbjørnsdottir case the EFTA court decided that a state can be held liable for an incorrect implementation of a Directive because of the homogeneity objective, the objective of establishing the right of individuals and economic operators to equal treatment and equal opportunities.[202] The dissenting opinion argues that the state liability is inseparable from the fundamental principle of the direct effect in the European Communities.[203] The principle of direct effect and State liability constitute complementary elements of the supranationality of Community law.[204] This supranationality is not part of the EEA-Agreement[205] because the EEA-Agreement was thought to be only an economical area.[206] The homogeneity clause has two foundations in the EEA-agreement.[207] On the one hand is the material provision of the EEA-Agreement largely identical to corresponding provisions of the ECT or the ECSC.[208] These provisions are incorporated into the national law of the member state.[209] On the other hand elaborates the EEA-Agreement mechanisms with a view to ensure a homogeneous interpretation and application of the incorporated material provisions.[210] The reason for these mechanisms is given in Recital 4 and 15 of the EEA-Agreement. Art. 6 EEA-Agreement is part of the mechanisms that should ensure homogeneity because it demands that those provisions of the EEA-Agreement which are in substance identical to that one of the EC Treaty and ECSC Treaty shall be interpreted according to the case law of the ECJ.[211] Art. 105 and 106 EEA Agreement establish a Committee that keeps under constant review the case law of the ECJ and the EFTA Court.[212] The objective to ensure individuals and economic operators equal treatment and equal

[201] Rt. 2005 1365 (52).
[202] EftaCourt E-9/97, 60.
[203] Efta Court, Case E-4/01, 26.
[204] Efta Court, Case E-4/01, 26.
[205] Efta Court, Case E-4/01, 26.
[206] See. Art. 1 (1), Rec. 4, 5, 6 EEA-Agreement.
[207] EftaCourt E-9/97, 52.
[208] EftaCourt E-9/97, 53.
[209] EftaCourt E-9/97, 53.
[210] EftaCourt E-9/97, 54.
[211] EftaCourt E-9/97, 54.
[212] EftaCourt E-9/97, 56.

conditions of competition as well as an adequate means of enforcement requires a homogenous interpretation of EEA-Law.[213]

Because of all this the EEA-Agreement is considered by the EFTA-Court to be an international treaty sui generis which contains a distinct legal order of its own.[214] As its scope goes beyond that what an agreement under international public law has, a Member State has to be hold liable for an incorrect implementation of a Directive.[215] Although the EEA-Agreement is not as far reaching in its depth of integration[216] and because of that the ECJ-Decision regarding the direct effect of directives is not applicable over Art. 6 EEA-Agreement[217] because they are based on special characteristics of European Community legal order which are not part of the EEA-Agreement,[218] Directives cannot be applied directly within the EEA.[219] Therefore the application of the principles for State liability as developed by the ECJ may not necessarily be in all respects coextensive.[220] The state is only held liable according to EFTA-Court judgements if three requirements are fulfilled:

- the Directive aims to give a subject individual rights[221]
- there is an incorrect implementation which is sufficient serious[222]
- the breach of EU/EEA Law causes a loss of an action[223]

### 6.3.1 Individual right of a subject

Within the ESD the first requirement is problematic because the Directive does not have effect between two private persons as it is not changing contract laws as the Directive states in Art. 1 ESD.[224] An individual right within the Directive might be the right to use an electronic signature

[213] EftaCourt E-9/97, 57.
[214] EftaCourt, E-9/97, 59.
[215] Efta Court, Case E-9/97, 59.
[216] Efta Court, Case E-9/97, 59.
[217] Efta Court, Case E-9/97, 44
[218] Efta Court, Case E-9/97, 44
[219] Efta Court, Case E-9/97, 66
[220] Efta Court, Case E-4/01, 30.
[221] Efta Court, Case E-9/97, 66; E-4/01, 32.
[222] Efta Court, Case E-9/97, 66; E-4/01, 32.
[223] Efta Court, Case E-9/97, 66; E-4/01, 32.
[224] The question if or if not a Directive has direct effect between two private persons is not so easy to answer and reaches beyond the scope of this work.

in the same way as a handwritten signature. That is the case when the relevant provision is unconditional and sufficiently precise.[225] To determine this three points are to be considered:[226]

- the identity of the persons entitled to the guarantee provided[227]
- the content of that guarantee[228] and
- the identity of the person liable to provide the guarantee.[229]

The non-discrimination rule of Art. 5 II ESD is a guarantee that electronic signatures are not discriminated out of the said reasons. It does not guarantee legal effectiveness as such but a minimal recognition for its legal effectiveness because an electronic signature cannot be held ineffective solely on the grounds that it is ineffective or does not fulfil the requirements of a qualified certificate.[230]

The persons who is entitled to this guarantee is everyone who uses an electronic signature because Art.5 II ESD protects a user of an electronic signature because only a user of an electronic signature needs to know what legal effect an electronic signature has. Art. 5 II ESD is precise and unconditional enough for a court to determine if someone uses an electronic signature and therefore a court is enabled to determine whether or not a person should be regarded as a person to benefit under the directive.

The person liable to provide that guarantee is the Member State as stated in Art. 5 II ESD because the Member State should install a legal system that makes it possible to use an electronic signature without the fear of rejection due to its electronic nature or non-fulfilment of a certain technology.

Therefore the ESD provides an individual right.

---

[225] Efta Court, Case E-9/97, 66; E-4/01, 32; ECJ, Francovich, 11; ECJ, Brasserie du Pecheur, 21.
[226] ECJ, Francovich 12.
[227] ECJ, Francovich 12.
[228] ECJ, Francovich 12.
[229] ECJ, Francovich 12.
[230] Encyclopedia of information technology law, 3.249/3.

### 6.3.2 Sufficiently serious incorrect implementation

The incorrect implementation must be sufficiently serious.[231] That depends on whether an EEA State has in the exercise of its legislative powers manifestly and gravely disregarded the limits on the exercise of its powers.[232] The factors that have to be determined for the conditions are the clarity and precision of the rule infringed, the measure of discretion left by that rule to the national authorities, whether the infringement and the damage caused was intentional or involuntary and whether any error of law was excusable or inexcusable,[233] the fact that the position taken by an EEA or Community institution may have contributed towards the omission and the adoption or retention of national measures or practices contrary to the EEA-Agreement.[234] These factors are determined by a national court.[235] The finding of a breach of EEA Law is not in itself determinative because a mere infringement of EEA law by an EEA State does not necessarily constitute a sufficiently serious breach.[236] A breach is considered to be sufficiently serious if it has persisted despite settled case law from which it is clear that the conduct in question constituted an infringement.[237] Such case law from the ECJ does not exist as the Commission report from 2006 states.[238] But there are some judgements courts in Slovenia and Finland where a discrimination of an electronic signature because it is electronic was dismissed.[239] These two decisions might give a hint that the ECJ will not tolerate any discrimination because Art. 5 II ESD states clear the reasons why an electronic signature cannot denied legal effectiveness but this is quite hard to predict.

Because this rule gives a very basic protection against a certain sort of discrimination it gives a lot of discretion to the national authority which legal effect an electronic signature has which is not a qualified signature according to Art. 5 I ESD. The Norwegian government saw quite

---

[231] Efta Court, Case E-4/01, 38, E-9/97, 69.
[232] Efta Court, Case E-4/01, 38, E-9/97, 69.
[233] Efta Court, Case E-4/01, 38, E-9/97, 69.
[234] Efta Court, Case E-9/97, 69.
[235] Efta Court, Case E-4/01, 38.
[236] Efta Court, Case E-4/01, 40.
[237] Efta Court, Case E-4/01, 40.
[238] Commission Report Com 2006, 5.
[239] Mason Electronic Signatures in Law, p. 144.

clearly that the non-discrimination rule was not implemented into Norwegian law[240] but they assumed that the principles of the free consideration of evidence as well as the freedom of giving evidence includes the non-discrimination rule. This is valid if one considers the admissibility of an electronic signature as evidence but not for the legal effectiveness of an electronic signature. Considering this breach if it was involuntary or intentional this seems to be intentional as the government clearly knew that it does not implement the non-discrimination rule of Art. 5 II ESD. But as the Norwegian government considered the non-discrimination rule of Art. 5 II ESD implemented through existing Norwegian Law this failure seems to be merely involuntary. In the light that the free considering of evidence includes a consideration of the legal effect it seems to be possible but unlikely that a judge denies solely a legal effect of an electronic signature because it is electronic or not a qualified signature while he is not denying the admissibility as evidence before court out of that reason. The principle of free consideration does not hinder such a result because it gives the judge the choice to decide what reasons he finds sufficient and thorough enough to consider evidence. The principle of free consideration makes such a consideration only mere improbable.

As stated above the legal effect of an electronic signature is not only found in court, it is effective outside the court as well and there is the chance as well that an electronic signature is discriminated by the legislator because of the reasons forbidden by Art. 5 II ESD.

These two points which are not implemented into Norwegian Law are part of the main provision of the ESD,[241] a discretion what the minimum recognition of an electronic signature is. An improbability that such discrimination is not happening is not sufficient enough to ensure a non-discrimination of electronic signatures according to Art. 5 II ESD because this ends in a legal uncertainty for the citizens. They, as legal lay persons, cannot foresee what the judge will consider as content of an electronic signature if the judge is considering the electronic signatures as evidence.

The aim of the ESD is to harmonise the legal recognition of electronic signatures to strengthen confidence in electronic signatures and the general appliance of them.[242] Divergent rules with

[240] Ot.prp.Nr. 82 (1999-2000), 8.10.2.
[241] Innst.O. nr. 41. 41 (2000-2001), 3.
[242] Rec. 4 ESD.

respect to the legal recognition are according to Rec. 4 ESD considered to hinder the free movement of goods because they create barriers in the use of electronic signatures. These barriers are considered to hinder the use of electronic communications and electronic commerce. This hinders to implement an internal market. As Rec. 20 ESD considers harmonised criteria for the legal effects of electronic signatures this will preserve a coherent legal framework across the Community. The aim of an internal market will be reached. The establishment of the internal market is according to Art. 1 EEA-Agreement the main aim of the Agreement. Therefore the missing implementation of the non-discrimination rule of Art. 5 II ESD can be considered to hinder the establishment of the internal market because the legal recognition of electronic signatures is not coherent with in the rest of Europe. A breach of such an important part of the ESD is therefore considered to be sufficiently serious.

### 6.3.3 Loss of an action

If or if not a case is lost because of this implementation can be just a presumption in this work. This seems unlikely but possible. Therefore Norway might be held liable for the missing implementation of the non-discrimination rule.

## 6.4 Non-Compliance of letter l) of Annex II ESD

The non-implementation of letter l) of Annex II ESD might constitute a breach of ESD law as well. The requirements in Annex II ESD for the certification-service-providers are mandatory. As the technology does not give the possibility to fulfil letter l) of the Annex II today, it seems to be not harmful to not implement that letter. But as Telenor pointed out in Otp prp. 82 (1999-2000) this might be a problem with further technological developments. Although it does not lead now to problems, it might cause problems with a further developed technology which makes subsequent changes in the certificate traceable because then the Norwegian implementation has created different rules for certificate-service-providers which might develop a barrier within electronic communication.

## 7 Conclusion

The ESA and the ESD have both established a system for legal recognition of electronic signatures. Both laws use the same three sorts of electronic signatures, electronic signatures, advanced electronic signatures and qualified signatures.

An electronic signature serves in both Laws the purpose of identifying someone via the form of an attachment of an electronic document while an advanced electronic signature has got stricter requirements as it should uniquely link to and identify a person, should detect alteration of the document and should be created by a device under the sole control of the signatory. The 'highest' form of a signature is the qualified signature, that is an advanced electronic signature that is based on a qualified certificate which fulfils certain information requirements and is issued by a qualified certification issuer who fulfils certain organisational, data protection and informational duties and is based on a secure signature creation device. Only qualified signatures are presumed according to both regulations to be equivalent with handwritten signatures. The electronic signatures should get a minimum protection against non-discrimination according to Art. 5 II ESD while the Norwegian solution is to allow an electronic signature maybe the same legal recognition as a qualified one in Section 6 S. 2 ESA. This approach serves very well the particular function a signature serves according to the respective legal requirement.[243] It gives the judges a very broad guideline about the content an electronic signature proofs. This 'functional' approach has got the same flexibility as the non-discrimination rule and is more elegant. The ESD gives no guidelines to the judges, only a prohibition what they should not consider as denial of a legal effect. But this Norwegian solution does not comply with the solution of the Directive because it allows discrimination. Although a non-discrimination in the field of the admissibility as evidence of an electronic signature is implemented in Norwegian Law through the principle of free giving of evidence the legal effect of an electronic signature can be denied if a judge

[243] Riisnæs, Digital Certificates and Certification Services, 3.7.

considers a general finding like the electronic format is sufficient enough to deny a legal effect for an electronic signature. The same problem occurs with the legal effect of an electronic signature outside of a court for the legislator. The legislator is free to discriminate electronic signatures because of the forbidden reasons because he can give exemptions to existing law. This means that a legislator can consider in a legislative act that an electronic signature is denied a legal effect because of its electronic format.

The question is what consequences such a breach of EEA-Law might have. As the EEA is not a supranational organisation like the EU a direct effect of the ESD must be denied because that would be an infringement of the sovereignty of an EEA-State. But if some requirements are fulfilled the breach can lead to a state liability as developed under EFTA-Court Law. The incorrect implementation of the non-discrimination rule is a sufficiently serious breach of the EEA-Agreement and the Directive confers an individual right to a subject because the ESD guarantees a user of an electronic signature a protection of his electronic signature against discrimination because it is electronic or not a qualified signature.

The third requirement, a loss of a case is not fulfilled yet, but this might happen. Under the condition that someone loses a case because the electronic signature he uses is discriminated out of the reasons laid down in Art. 5 II ESD, Norway would be liable for that loss. If such a case happens in reality, only time will tell. From a European perspective the incorrect implementation of Art. 5 II ESD harms if it hinders to reach the goals the ESD wants to achieve. As Rec. 4 ESD states should the ESD strengthen the confidence in and the general acceptance of electronic signatures with clear rules regarding the legal recognition of them. Divergent rules for the legal recognition create a significant barrier to the use of electronic communications and electronic commerce. This will be hindering the free movement of goods and services of the internal market. To create a European internal market is the main reason why the EEA was established, see Art. 1 EEA Agreement. From a European perspective this implementation hinders the establishing of an internal market with respect to electronic communications and e-commerce because the minimum of legal recognition of an electronic signature is not guaranteed in Norway.

## References


List of Judgements/Decisions

ECJ

ECJ, Brasserie du Pecheur

ECJ, Francovich

Efta Court

Eftacourt E-9/97 (Sveinbrøttodir)

Eftacourt E-4/01 (Karlsson)

Høysterett

Rt. 2000-1826 (Finanger I)

Rt. 2005-1690 (Finanger II)

Rt. 90-1008

Other

TOBYF 2004-598

BGH, XI ZR 210/03 http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=16fc52b819a4afa6c7643793306a15dd&client=13&nr=30741&pos=0&anz=1

OLG Stuttgart, NJW-RR 2002, 1274 -1276

Treaties/Statutes

EEA-Agreement

Electronic Signatures Directive

Norwegian Electronic Signatures Act

Tvisteloven

Straffeprosessloven

EØS-Loven

BGB

Secondary Literature

Statutory documents

European Union

EU-Commission Report; COM 2006/120 final

Commission action Plan, COM (2008) 798 final

Found on: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF; visited 15/07/2009

Commission decision 2003/511/EC

Found on: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32003D0511&model=guichett; visited 15/07/2009

CWA 14169:2004

Found on: https://www.cen.eu/CENORM/Sectors/sectors/isss/cen+workshop+agreements/cwa_listing.asp; visited 15/07/2009

Working Paper, found on  Mason, Electronic Signatures in Law, p. 150

Norway

OT.prp.Nr. 82, found on: http://www.regjeringen.no/Rpub/OTP/19992000/082/PDFA/OTP199920000082000DDDPDFA.pdf; visited: 28.07.2009.

Annex to Innst.O. nr. 41. 41 (2000-2001) found on: http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Odelstinget/2000-2001/inno-200001-041/?lvl=0; visited: 28.07.2009.

Innst.O. nr. 41. 41 (2000-2001) found on: http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Odelstinget/2000-2001/inno-200001-041/?lvl=0; visited: 28.07.2009.

Books

| | |
|---|---|
| Andenæs, Johs | Norsk Straffeprosess<br>Bind 1<br>3rd edition, Oslo 2000<br>Quot.; Andenæs, |
| Brazell, Lorna | Electronic Signatures Law and Regulation<br>London, 2004<br>Quot: Brazell, Rn. |

| | |
|---|---|
| Dumortier, Jos | The Legal Aspects of Digital Signatures,<br>Executive Summary<br>Summary of the Reports<br>Table of contents<br>Gent, 1998,<br>Quot.: Dumortier, The Legal Aspects of Digital Signatures,<br>Vol. I, p. |
| Dumortier, Jos | The Legal Aspects of Digital Signatures,<br>Introductory Report: The Digital Signature:<br>Technical and Legal Issues,<br>Gent, 1998,<br>Quot.: Dumortier, The Legal Aspects of Digital Signatures,<br>Vol. II, p. |
| Dumortier, Jos | The Legal Aspects of Digital Signatures,<br>ReportV: Solutions?<br>Gent, 1998,<br>Quot.: Dumortier, The Legal Aspects of Digital Signatures,<br>Vol. VI, p. |
| Dumortier, Jos; Kelm, Stefan<br>Nilsson, Hans; Skouma, Georgia<br>Van Eecke, Patrick | The Legal and Market Aspects of Electronic Signatures,<br>Final report, 2003,<br>found on<br>http://www.epractice.eu/files/media/media_581.pdf<br>Quot: Dumortier, The Legal and Market Aspects of<br>Electronic Signatures, p. |

| | |
|---|---|
| Feghhi, Jalal, Feghhi, Jalil<br>Williams, Peter | Digital Certificates Applied Internet Security,<br>Addison Wesley Longman Inc,. Reading 1999<br>Quot: Feghhi, Feghhi, Williams, Digital Certificates, p. |
| Hustad, Knut-Fredrik;<br>Øydegard, Johan; Dahl, Arne Willy;<br>Haug, Ved Stig-Ole;<br>Thorheim, Karl Otto; Skaflem, Ingolf;<br>Haugland, Geir Sunde; | L 22.05.1981 nr. 25 Lov om rettergangsmåten i straffesaker (Straffeprosessloven)<br>Gyldendal rettsdata,<br>last updated: 17.08.2009<br>Quot.: Commentator, 1. |
| Mason, Stephen | Electronic Signatures in Law,<br>2nd edition, London, 2007<br>Quot.: Mason, Electronic Signatures in Law, P. |
| Saxby, Stephen | Encyclopedia of information technology Law<br>Volume I<br>London 2001<br>Quot.: Encyclopedia of information technology Law, Rn. |
| Schei, Tore; Bårdsen Arnfinn;<br>Nordén, Dag Bugge;<br>Reusch, Christian H.P.;<br>Øie Toril M | Tvisteloven (lov av 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister), Kommentarutgave<br>found on:<br>http://www.kommentarutgaver.no/page/mainpage3.jsp,<br>visited: 25.08.2009.<br>Quot: Schei, §, 1. |
| Schellekens, M.H.H. | Electronic Signatures<br>Authentication Technology from a Legal Perspective<br>The Hague 2004<br>Quot.: Schellekens p. |

Essays

Bell, Josh; Gomez, Ruben; Hodge, Paul; Mayer-Schönberger, Viktor
Electronic Signature Regulation An early scorecard – comparing electronic signatures legislation in the US and the European Union
in: Computer Law & Security Report Vol. 17, p. 399 - 402
Quot.: Bell, Gomez, Mayer-Schønberger, Electronic Signature Regulation, CLSR Vol. 17, 399 (p.).

Bratholm, Anders,
Den straffeprosessuelle betydning av at et bevis er skaffet til veie på ulovelig mate
In: Tidsskrift for rettsvitenskap 1959 S. 109
Quot.: Anders Bratholm, TFR-1959-109

Fischer- Dieskau, Stephanie; Gitter, Rotraud; Paul, Sandra; Steidle, Roland
Elektronisch signierte Dokument als Beweismittel im Zivilprozess
in: MMR 2002, 709 – 713.
Quot.: Fischer-Dieskau, Gitter, Paul, Steidle, MMR 2002, 709 (p.)

Harbo, Tor-Inge
The European Economic Area Agreement: A Case of Legal Pluralism
In: Nordic Journal of International Law 78 (2009) 201 - 223
Quot.: Nordic Journal of International Law 78 (2009) 201 (p).

Kindl, Michael; Werner, Dennis
Rechte und Pflichten im Umgang mit PIN und TAN
Computer und Recht, 2006 353 – 360
Quot.: Kindl/Werner CR 2006, 353 (p).

| | |
|---|---|
| Kuner, Chris; Baker, Stewart; Barcelo, Rosa; Greenwald, Eric | ILPF working paper, Found on: http://www.ilpf.org/groups/analysis_IEDSII.htm, visited: 24.11.2009 Quot.: Kuner, ILPF working paper, on: http://www.ilpf.org/groups/analysis_IEDSII.htm, visited: 24.11.2009. |
| Nordén, Anna | Electronic Signatures in a legal context In: Cecilia Magnusson Sjöberg, IT Law for IT Professionals – an introduction Lund, 2005 Quot.: Nordén Electronic Signatures in a legal context, 1.1. |
| Nordén, Anna; Sjöberg, C. Magnusson | Managing Electronic Signatures – Current Challenges in: IT-Law, edited by Peter Wahlgren Stockholm, 2004 Quot.: Sjöberg, Nordén, Managing electronic Signaturs, p. |
| Reed, Chris | What is a Signature? In: Journal of Information, Law and Technology, 2000 (3) Found on: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ Visited: 09.12.2009 Quot.: Reed, What is a signature, 1.1. |

| | |
|---|---|
| Riisnæs, Rolf | Digital Certificates and Certification Services,<br>in: IT-Law, edited by Peter Wahlgren<br>Stockholm, 2004<br>Quot.: Riisnæs, Digital Certificates and Certification Services, 1.1 . |
| Schymik, Carsten | Norwegens Sonderweg nach Europa, Warum Norwegen nicht Mitglied in der Europäischen Union ist.<br>C-173 on<br>http://www.zei.de/zei_deutsch/publikation/publ_zeic_dp.htm<br>Visited: 22.09.2009.<br>Quot.: Schymik, Norwegens Sonderweg nach Europa, p. |
| Sinsi, Vincenzo | Digital Signature Legislation in Europe<br>in: International Business Lawyer 2000, 487<br>Quot.: Sinsi Digital Signature Legislation in Europe, International Business Lawyer 2000, 487 (p). |
| Thorvaldsen, Kjell;<br>Skomedal Åsmund;<br>Ericson, Trond | Bevisverdien av elektronisk informasjon<br>in: Revisjon og Regnskap, utgave 4/2007<br>Quot.: Thorvaldsen, Skomedal, Ericson, Revisjon og Regnskpap, 4/2007 p. |
| Wang, Minyan | Do the regulations on electronic signatures facilitate international electronic commerce? A critical review<br>in: Computer law & Security Report Vol. 23 p. 32 – 41<br>Quot.: Wang; Critical review; CLSR; Vol. 23, 32 (p). |

Others

RFC 5280

www.smartcardbasics.com, visited: 21.07.2009.

Unofficial translation by http://www.npt.no/ikbViewer/Content/1379/1379-electronic_signatures_act.pdf; visited 23.07.2009

A