CEN

WORKSHOP

AGREEMENT

CWA 14365-1

March 2004

ICS 03.160; 35.040; 35.240.60

Supersedes CWA 14365:2003

English version

Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Contents ... 2
Foreword ... 3
1 Scope ... 4
2 References ... 5
2.1 Normative References ... 5
2.2 Informative References ... 5
3 Definitions and abbreviations ... 7
3.1 Definitions ... 7
3.2 Abbreviations ... 7
4 Signatures from a technical and legal perspective ... 9
4.1 Technical Definitions of Security Services ... 9
4.2 Signatures from a legal perspective ... 10
4.2.1 Technical and legal aspects ... 10
4.2.2 Signatures from a functional perspective ... 11
4.2.3 The need for non-technical evidence ... 11
4.2.4 Features of functional signatures ... 12
5 Comparison of signature definitions ... 14
5.1 Digital signature definition ... 14
5.2 Electronic Signature definition ... 15
5.3 Advanced Electronic Signature definition ... 16
5.4 Qualified Electronic Signature definition ... 17
Legal Relevance of Different Types of Electronic Signature ... 18
6 Use Cases for Non-Qualified Electronic Signatures ... 20
6.1 The Components of Qualified Electronic Signatures ... 20
6.2 Advanced Electronic Signature without SSCD ... 21
6.3 Advanced Electronic Signature without Qualified Certificate ... 23
6.4 Digital Signature without Data Representation ... 23
7 Evidence for electronic signatures ... 25
7.1 Evidence present in the signed data ... 25
7.2 Evidence present in the certificate ... 26
7.3 Evidence present in the Certificate Policy and/or CPS ... 26
7.4 Evidence regarding Certificate Status ... 26
7.5 Evidence present in the Signature Policy ... 27
7.6 Evidence at the Registration Authority ... 27
7.7 Evidence not available through the signed message ... 28

Foreword

Successful implementation of European Directive 1999/93/EC on a Community framework for electronic signatures [Dir.1999/93/EC] requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products.

In 1999 the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players, to create the European Electronic Signature Standardisation Initiative (EESSI).

Within this framework the Comité Européen de Normalisation / Information Society Standardisation System (CEN/ISSS) and the European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI) were entrusted with the execution of a work programme to develop generally recognized standards to support the implementation of [Dir.1999/93/EC] and development of a European electronic signature infrastructure.

The CEN/ISSS Workshop on electronic signatures (WS/E-SIGN) resulted in a set of deliverables, CEN Workshop Agreements (CWA), which contributed towards those generally recognized standards. The present document is one such CWA.

The purpose of this CWA is to give guidance on the use of electronic signatures. Whilst the focus often has been on "qualified electronic signatures" as specified in Article 5.1 of the Directive, a side effect was that the requirements of employing general electronic signatures (referred to as "5.2 signatures") in e-commerce were not sufficiently addressed.

The purpose of this part of the CWA is therefore to describe the general legal and technical aspects of electronic signatures, and thus extend the work to e-commerce scenarios, paying special attention to technologies with a high deployment capacity, to enable trust, without the need to meet all the strict requirements for "Article 5.1 Signatures".

This part of the CWA is intended for use by both legal and technical experts in the area of electronic signatures, as well as designers of systems and products in this area.

The CWA consists of the following parts:

- Part 1 - Legal and technical aspects (this part)
- Part 2 - Protection Profile for Software Signature-Creation Devices

This version of this CWA Part was published 2004-03.

A list of the individuals and organizations which supported the technical consensus represented by this CEN Workshop Agreement is available to purchasers from the CEN Central Secretariat.

1 Scope

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures [Dir.1999/93/EC] – referred to as the Directive in the remainder of this document – established a legal framework for electronic signatures and certification-services in order to contribute to their legal recognition. It is laid down in article 5.1 that electronic signatures fulfilling certain quality metrics – so called qualified electronic signatures – satisfy the requirements of handwritten signatures. In article 5.2 a residual provision is given where electronic signatures are not denied legal effectiveness and admissibility as evidence in legal proceedings, even if the quality metrics of qualified electronic signatures are not met.

The scope of this document is on the latter –electronic signatures that do not fulfil all the requirements laid down for qualified electronic signatures in article 5.1 of the Directive. The document therefore analyses the differences between cryptographic mechanism of digital signatures, qualified electronic signatures (according to article 5.1 of the Directive), and electronic signatures (according to article 5.2 of the Directive). In addition, a set of use cases of electronic signatures which do not fulfil some of the requirements laid down in article 5.1 are discussed in order to point out its effectiveness in e-commerce environments or in various application fields asking for authentication measures.

In addition to the use cases, the evidence that is provided by electronic signatures is discussed. The electronic signatures and certification-services are broken up into its basic elements and the proof provided by each element is discussed from a legal perspective in order to establish the coherence between the technical elements and its legal effect.

Part 2 of this CWA contains a Protection Profile (PP) for a Software Signature Creation Device [SCDev-PP] suitable for such general electronic signatures. This Protection Profile follows the provision of the Common Criteria (CC) [ISO 15408]. It is based on the [SSCD PP] that has been developed as a standard for devices that are capable of creating qualified electronic signatures.

Although a CC PP has been chosen for highlighting the added value of independent evaluation of the security measures provided by the SCDev, other evaluation criteria may serve that purpose as well. Examples of such criteria are [FIPS 140-2] or [ITSEC].

2 References

2.1 Normative References

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this CWA are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to apply.

[Dir.1999/93/EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures.

[SSCD PP] CEN/ISSS WS/E-Sign Workshop Agreement 14169: Security Requirements of Secure Signature Creation Devices (SSCD), March 2002

[SCDev-PP] CEN/ISSS WS/E-Sign Workshop Agreement 14365-2: Protection Profile for Software Signature-Creation Devices.

[ISO 15408] ISO/IEC 15408-1 to 15408-3: Information technology - Security techniques - Evaluation criteria for IT security – Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements, 1999.

2.2 Informative References

[CWA 14170] CEN/ISSS WS/E-Sign Workshop Agreement 14170: Security Requirements for Signature Creation Applications.

[CWA 14171] CEN/ISSS WS/E-Sign Workshop Agreement 14171: Procedures for Electronic Signature Verification.

[EEC 1980/934] Convention on the law applicable to contractual obligations opened for signature in Rome on 19 June 1980, 80/934/EEC, Official Journal L266.

[FIPS 140-2] NIST: Security Requirements for Cryptographic Modules, Federal Information Processing Standard FIPS PUB 140-2, 2001.

[HCCH] Hague Conference on Private International Law: Status of the Hague Conventions, online avail. at http://www.hcch.net/

[ISO 10181-2] ISO/IEC 10181-2: Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework, 1996.

[ISO 10181-4] ISO/IEC 10181-4: Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework, 1997.

[ISO 13888-1] ISO/IEC 13888-1: Information technology - Security techniques - Non-repudiation - Part 1: General, 1997.

[ISO 7498-2] ISO 7498-2: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989.

[ITSEC] Commission of the European Communities: Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, 1991.

[TS 101456] ETSI: Policy requirements for certification authorities issuing qualified certificates, TS 101 456, v1.1.1, January 2002.

[TS 101733] ETSI: Electronic Signature Formats“, ETSI TS 101 733, v1.2.2, December 2000.

[TS 101862] ETSI: Qualified Certificate Profile, ETSI TS 101 862, v1.2.1, June 2001.

[TS 101903] ETSI: XML advanced Electronic Signatures, ETSI TS 101 903, v1.1.1, February 2002.

[TS 102 038] ETSI: XML Formats for Signature Policies, ETSI TR 102 038 v0.0.3, December 2001.

[UNCISG] United Nations: United Nations Convention on Contracts for the International Sale of Goods, 1980.

[SMIME] B. Ramsdell: S/MIME Version 3 Message Specification, RFC 2633, 1999.

[SSL] A.O. Freier, P. Karlton, P.C. Kocher: SSL Protocol, Version 3.0. Netscape Communications Corp., 1996.

[TLS] T. Dierks and C. Allen: The TLS Protocol Version 1.0, RFC 2246, 1999.

3 Definitions and abbreviations

3.1 Definitions

‘Qualified electronic signature’ means an electronic signature that fulfils the requirements laid down in the Directive [Dir.1999/93/EC] article 5(1), i.e. an advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device.

Directive: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999on a Community framework for electronic signatures in OJ EC 19.1.2000, L12/12

3.2 Abbreviations

AS	Advanced electronic Signature
CC	Common Criteria Version 2.1
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CGA	Certification Generation Application
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
EC	European Commission
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
ETSI SEC	ETSI Security Technical Committee
HI	Human Interface
HW	Hardware
I/O	Input/Output
ISSS	Information Society Standardisation System
NRO	Non-Repudiation of Origin
OCSP	Online Certificate Status Protocol
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant

PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKIX	Public Key Infrastructure (X.509)
PP	Protection Profile
QC	Qualified Certificate
RAD	Reference Authentication Data
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SCA	Signature-Creation Application
SCD	Signature-Creation Data
SCDev	Signature Creation Device
SDO	Signed Data Object
SFP	Security Functional Policy
SFR	Security Functional Requirement
S/MIME	Secure Multi-Purpose Mail Extension
SOF	Strength of Function
SSCD	Secure Signature-Creation Device
SSL	Secure Socket Layer
SVD	Signature-Verification Data
TLS	Transport Layer Security
TOE	Target of Evaluation
VAD	Verification Authentication Data
WS/E-SIGN	CEN/ISSS Electronic Signatures workshop

4 Signatures from a technical and legal perspective

In order to discuss the different types of electronic signatures later in this document, it is useful to first take a look at the ISO definitions relating to the security services which are using the digital signature mechanism: authentication, data integrity and non-repudiation (Section 4.1).

Moreover, it is necessary to also take into consideration the four basic types of signatures that can be seen from the legal perspective (Section 4.2).

4.1 Technical Definitions of Security Services

Authentication: The provision of assurance of the claimed identity of an entity [ISO/IEC 10181-2].

Data origin authentication: The corroboration that the source of data received is as claimed [ISO 7498-2].

Peer entity authentication: The corroboration that a peer entity in an association is the one claimed [ISO 7498-2].

Data integrity: The property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2].

Repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication [ISO 7498-2].

Non-repudiation of origin: This service is intended to protect against the originator's false denial of having created the content of a message and of having sent a message [ISO/IEC 13888-1].

Non-repudiation: This service is intended to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence or the non-occurrence of the event or action [ISO/IEC 10181-4].

For **authentication**, it is important to point out that there are actually two different types of authentication services: data origin authentication and peer-entity authentication.

Data origin authentication, in the context of this document, is related to the transmission of signed messages, which can be verified by the receiver at a later point in time. Data origin authentication is therefore the service which most closely relates to the general definition of “electronic signature” in the Directive, as described in the next chapter. An example of using the digital signature mechanism for this purpose is signing e-mail using the S/MIME protocol.

Peer-entity authentication relates to the authentication of a communicating party in an on-line session. An example of using the digital signature mechanism for this purpose is client and server authentication using the secure socket layer [SSL] or transport layer security [TLS] protocol.

Data integrity ensures that changes in transmitted data can be detected, irregardless of if this is due to a malicious attacker or due to transmission errors. An example of using the digital signature mechanism for this purpose is once again signing e-mail using the S/MIME protocol.

For **non-repudiation**, [ISO 7498-2] and [ISO/IEC 13888-1] define several types of non-repudiation services. A general definition of non-repudiation service is given in [ISO/IEC 10181-4]. The one usually associated with electronic signatures is actually defined as “non-repudiation of origin”. When applying this definition, we should bear in mind that “having created the content of the message” refers to the signature created by the signatory, and not necessarily the document being signed. Non-repudiation of origin (NRO) is also the service that most closely relates to the definition of Qualified Electronic Signatures (“5.1 signatures”) in the Directive, described later in this document. Of course the NRO service does not prevent a signatory to later deny his signature; it only makes it much more difficult for him to prove this in case of a dispute, and in some legal systems, the NRO service even implies a presumption that the signature is genuine. An example of using the digital signature mechanism for this purpose is signing a legally binding contract, fulfilling all the security requirements of a qualified electronic signature.

4.2 Signatures from a legal perspective

4.2.1 Technical and legal aspects

Data integrity, peer to peer authentication and data origin authentication as discussed in the previous section are purely technical definitions taken from technical standards. To assess the services provided by their technical implementation from a legal perspective, we have to rely on the scientific and technologic evidence in order to verify:

a) if a signature is authentic, i.e.
- it corresponds to a specific person, and
- it is not forged

b) if the signed data is original, i.e.
- it corresponds to the data presented to the signer, and
- it has not been altered.

Non-repudiation is a more complex service, and there the technology has to be complemented with the legal concept of non-repudiation. Non-repudiation in legal environment does not only apply to the signature itself, but also to verbal declarations and to behaviours.

In legal terms, the non-repudiation of a signature is determined:

a) by the applicable law, in open communities, and/or

b) by agreement, in specified communities that can be open or closed, depending on their policy.

The elements of legal non-repudiation are also different depending on the function of the signature and on the type of signed document/data. They can be distinguished in three different types:

a) non semantic (i.e. purely technical) elements, like authenticity, integrity,

b) contextual or semantic elements, subject to both technical and legal assessments, like knowledge, wilfulness, intention, understanding, interpretation, violence, error, deception, acting incapability etc,

c) purely legal elements, like legal validity/invalidity, legal capability/incapability, empowerment,

A technical definition of non-repudiation, which is made without taking into account the legal elements of non-repudiation provided by the applicable law and/or contractual agreement, is misleading and unusable for human activity. Stated further, if all technical evidences are in place, the parties still may not have sufficient information to create a binding contract.

The legal aspects of the signature functionality are not dependent on the level of trustworthiness. A document written and signed on paper with a pencil is a valid document regardless of the level of trustworthiness of paper and pencil. It is always better to have the functionality matched with an appropriate level of trustworthiness. However, from a legal perspective, the signature functionality is (or can be) still available. There is no logical or automatic equivalence between the technical and the legal definition of non repudiation. Even if the technical features of a signature are not fully adequate (testament written on a rock; written agreement executed and signed on a paper napkin), the signature can be considered legally relevant. Article 5.2 of the Directive correctly stipulates that electronic signatures shall not be discriminated for their technical weakness, and shall be admitted as a possible evidence, in the same way as today's technically weak handwritten signatures are admitted as evidence.

4.2.2 Signatures from a functional perspective

Based on the specific characteristics of signatures from a legal perspective, the following definitions describe the four basic functions of signatures – identification signatures, authentication signatures, signatures as declaration of knowledge, and signature as declaration of will. When using the digital signature mechanism, all signatures below (except for identification) also provide data integrity.

A. Signatures for Identification: This signature coincides with the ISO definition of peer-entity authentication. An example of such a signature is the challenge/response in client/server authentication used by protocols such as SSL and TLS. In that case, no document is signed; only a meaningless "nonce" is signed to provide "proof-of-possession" of the private key. This is most often not regarded as an "electronic signature" in the terms of the Directive, since it is not related to any data, but only as a specific usage of the "digital signature" mechanism.

B. Signatures for Authentication: This signature coincides with the ISO definition of data origin authentication, provided data is considered as an object and not as a document, with a specific semantic meaning. (If the signed data has a specific semantic meaning which the signature is set to confirm, we have a Signature for declaration of knowledge and/or will.) The signature is only meant to authenticate that the message originates from the stated sender. It does not by itself imply that the sender in any way approves the contents of the message, and can be fully automated without human interference or consciousness.. An example of such an electronic signature is the S/MIME signature used in many e-mail applications.

C. Signatures for declaration of knowledge: This type of signature is somewhere in a grey zone between the previous and the following signature type. This signature also represents data origin authentication (according to the ISO definition), but where data also has a semantic relevance. The knowledge of the semantic meaning of the signed data is necessary, but there is no need for a specific will/intention of the signer; normally the fact that a declaration has been signed is sufficient. Sometimes from the legal perspective it is not relevant if a signature was wilfully performed, it is only relevant that the signature is authentic and that the signed document delivers true information. In such cases the signature creation procedure is irrelevant as such: it does not matter if there was error, violence of deception. It only matters that the signature and the content of the document are true. In other words: when this type of signature is being used, this means that the signer declares that he has taken knowledge of the semantic meaning of the signed data but this does not mean that he approves the signed data. There is no specific will from the signer. This signature can be supported by the non-repudiation service (according to the ISO definition) with a specific indication included in the signed data elements to declare the intent of the signature: declaration of knowledge. Other possible tools can be provided by the IT infrastructure, in order to make recognizable that a declaration of knowledge is signed.

D. Signatures as declaration of will: This signature represents non-repudiation (according to the ISO definition), where data has a semantic relevance and describes a claimed event or action. However, because the signature expresses a specific will of the signer, not only the knowledge of the semantic content is necessary, but also a proper understanding of the signature creation (semantic and procedural) context. Such a signature must therefore be generated under the full control of the signer.

4.2.3 The need for non-technical evidence

In the paper-based world the meaning and function of a signature is assessable through:

- The physical context of the signature (on what kind of support it is attached, the semantics of the support etc.). The physical context of the signature is self-evident and needs (normally) no technical tools to be verified and assessed

- The semantic context of signature creation (time, place and other environmental conditions under which the signature has been created). Normally such information is made available either through the signed support or through witnesses.

- The semantic context of signature verification (time, place and other environmental conditions under which the signature has been verified). Normally the context of such verification is a legal facility (court, law firm, etc.)

In the digital world neither the physical context of the signature, nor the signature creation nor the verification context are self evident. Witnesses are normally not available, considering that the common use of electronic signatures is performed remotely (transactions at distance). This means that the only electronic signature that is able to carry (as such) as much evidential information as a handwritten one is an electronic signature, which has a relevance independent of the semantic of the signed data and of the signature creation and verification context. The only such electronic signatures are the identification and authentication signatures.

For electronic signatures as declarations of knowledge or as declarations of will, more information is needed in order to properly assess them. In the context of EESSI, the ETSI specifications on the qualified certificate profile [TS 101862], the specifications on policy requirements for CSPs [TS 101456], signature policies [TR 102 038] and electronic signature formats [TS 101 733] [TS 101 903], and the CEN specifications for signature creation [CWA 14170] and signature verification [CWA 14171] address such issues to a certain extent.

The signature creation and validation process for handwritten signatures has been highly informal for the last century. The corresponding specifications for electronic signatures formalise and structure the processes and therefore cannot address all possible contexts and signature relevance, used and accepted in the legal world today.

4.2.4 Features of functional signatures

The table at the end of this chapter shows the complexity of human activity in relation to the four envisaged functionalities of human signatures.

To understand the table, which refers to both handwritten and electronic signatures, it is necessary to be aware of the significant differences between handwritten signatures and electronic signatures. Such differences have a determinant influence on how the signature creation process can be assessed from a legal/functional perspective:

- The handwritten signature process is perceived, influenced and controlled directly through the human senses (sight, tact, hearing, speech); the only tool used in such a process has not autonomous functionalities and is totally passive in the hands of the signer. The electronic signature creation process is much more complex and is represented to the signer and controlled by the signer only through a highly complex infrastructure that in its whole is never under his/her sole control. The signer has control, possibly, only on the SCDev, which is (normally) only one of the many components needed to perform an electronic signature.

- The handwritten signature creation process at distance always is apperceived as such by the signer and has a completely different ritual (and is differently assessed from the legal perspective) than a co-located handwritten signature creation process. The electronic signature creation process does not so much differ, if carried out at distance or co-located, besides the possibility of personal biometric identification of the parties involved: the fundamental difference is made by the security features and the openness of the IT infrastructure on which it is carried out. From an abstract point of view, the IT infrastructure can rebuild all features of a co-located signature, including biometric identification, even enhancing the reliability of the signature creation process, compared to that of the co-located handwritten signature.

- Witnesses work properly in the handwritten signature creation process if such process is co-located: in fact a witness is useful in legal terms if it has a full and direct perception of any fact or activity that is legally relevant. If handwritten signatures are created at distance, the witness should also be the carrier of the DTBS in order to be an effective witness. The witness of electronic signatures has to be aware of two series of facts, in order to be effective: a) the way the IT infrastructure used to perform the signatures has worked; b) the human activity of the signers and its context. The way data has been carried is relevant only if the technical features of the created signatures are very weak.

All the above mentioned differences do not matter in order to verify the technical qualities of the signatures.They also are irrelevant from the perspective of technical non repudiation: in fact technical non repudiation is about collecting irrefutable evidence to resolve disputes about the occurrence or non-occurrence of the declaration of will that has been originated under a particular name contained in a public key certificate. It is not possible to infer from technical non repudiation the consequence of legal non repudiation. As clarified in Chapter 4.2.1, the validity of a signature from a legal perspective is not dependant (solely) on its technical quality, but on the quality of the context of the signature creation process and on the personal qualities (knowledge, free will, mental capacity, etc.) of the signer. The technical quality of the signature is just a minor issue in the process of legal assessment of a signature.

However, the influence of the context on the functional meaningfulness and on the legal relevance of a signature differs significantly, depending on what is the specific function of such a signature. Again these differences barely matter from a purely technical perspective.

The following table is a useful tool in order to understand the different interaction between context, semantics and signature creation process.

	AUTHENTICATION SIGNATURE	**SIGNATURE AS DECLARATION OF KNOWLEDGE**	**SIGNATURE AS DECLARATION OF WILL / INTENTION**
1. Identity	I know who I am	I know who I am	I know who I am
2. Place	I know where I am[1]	I know where I am[1]	I know where I am[1]
3. Data	Data may have meaning	Data has meaning	Data must have meaning
4. Context of signature creation	The data participates in the process	The data participates in the process and possibly the signer also	The data participates in the process and the signer must also
5. Knowledge of data	I may understand the meaning of the data	I understand the meaning of the data and …	I understand that the meaning of the data is compliant with my intention and …
6. Specific Intention	Irrelevant	… therefore I want to sign	… therefore I want to sign
7. Awareness of process	Optional	Mandatory	Mandatory
8. See what I sign	It may be necessary that I see what I sign	It is necessary that I see what I sign	It is necessary that I see what I sign
9.Act of signing	Signer may be passive	Signer is active	Signer is active
10. Link to data in process	There is a link between the signer and the data Both are relevant as facts.	There is a link between the signer and the data Both are relevant as facts Semantics are relevant in the signature creation context	There is a link between the signer and the data Both are relevant as facts Semantics are relevant in the signature creation context
11. Fully Functional	Yes	No – Additional acts may be necessary	No – Additional acts are normally required

5 Comparison of signature definitions

5.1 Digital signature definition

The term “digital signature” generally refers to a mechanism aiming at securing and validating the origin and the integrity of electronic data.

> **ISO 7498-2:1989**
>
> **Digital signature**: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source of the data unit and protect against forgery, e.g. by the recipient

With this definition, the digital signature mechanism can be used to secure electronic data units in various contexts. The signer/recipient of the data unit does not necessarily have to be a human being: it can be a hardware device, a computer programme or any other object. Imagine for example the communication between a mainframe computer and the measuring instruments of a weather forecast agency where sensors send data to the mainframe via a satellite connection. For this kind of application, digital signatures can be used as a mechanism to secure the transmission of data from the devices in the network. It is an application of digital signatures in an environment where the communication doesn’t occur between human beings but between machines. In a similar way, digital signatures can be used to verify the origin and the integrity of a Java applet activated between a server and a client on the Internet, or to secure images produced by road traffic speed control cameras. Digital signatures can also control the authenticity and the integrity of software patches exchanged via the Internet. In a similar way digital signatures can be used between human beings to provide data origin authentication, data integrity and non-repudiation.

Contrary to some signature laws, the ISO-definition does not restrict a digital signature to the use of *asymmetric* cryptography, although this is the predominant technology in use today. However, when using asymmetric cryptography with digital signatures, two major properties are not provided by the digital signature mechanism:

- knowing the owner of the public key
- knowing that private key was in the sole control of the signer at the time of the signature

The first property is usually provided by using public key certificates. The second property may for example be provided by using certificate status information (CRL or OCSP) with either time-stamp tokens or time-marks.

In order for a digital signature based on a public key certificate to be considered technically valid (according to the ISO definition of digital signature), it must be proven that the digital signature was applied while the signer's certificate was valid. Since in many cases relying on a time indicated by the signer or knowing when a signature has been created is not possible, an upper limit time may be used which is obtained by using a time-stamp token or a time-mark applied to a digital signature:

- A time-mark is a record in a secure audit trail, which includes at least a trustworthy time value and a hash representation of the datum.
- A time-stamp token is a signed data structure issued by a Time-Stamping Authority, which includes at least a trustworthy time value and a hash representation of the datum.

In case time-stamps or time-marks are used, to prove that the digital signature was generated while the signer's certificate was valid, the digital signature must be verified and the two following conditions satisfied:

- The time-stamp token or the time mark must have been applied before the end of the validity period of the signer’s certificate.

- The time-stamp token or the time mark must have been applied either while the signer’s certificate was not revoked or before the revocation date of the certificate.

5.2 Electronic Signature definition

> **Article 2 of 93/1999/EC**
> **Definitions**
>
> For the purpose of this Directive:
>
> 1.‘electronic signature ’means data in electronic form **which are attached to or logically associated with other electronic data** and *which serve as a method of authentication*;
>
> 2. ‘advanced electronic signature ’means an electronic signature which meets the following requirements:
>
> (a) it is uniquely linked to the signatory;
>
> (b) it is capable of identifying the signatory;
>
> (c) it is created using means that the signatory can maintain under his sole control; and
>
> (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

An Electronic Signature is data attached to or logically associated with (so called detached signatures) other electronic data having the function to establish a link between the signed data and a person. This link can serve just to assess presence in front of the data, knowledge of the data, acceptance of the data, declaration of the data, and/or origin/production of the data. The electronic signature is thus a digital procedure set to confirm a possible legal relevance of data for a specific person or group of persons. The exact semantics of the electronic signature has to be specified by some other means.

EU Member States are obliged, according to art. 5.2 of the Directive, to allow legal relevance of electronically signed data. The Directive creates the category of “Electronic Signatures” in order to define a legal framework for legal relevance of any technical mean to sign, validate, endorse and accept digital data.

“Electronic signature” is thus basically a legal concept, and thus electronic signatures exist only where legal relevance of digital evidence is admitted by the legal system.

In legal science the difference between a fact and a wilful act is commonly accepted. In each legal system the border between the two can have significant differences. Nonetheless the difference between a document with a signature which is relevant as a wilful act, and a document which can only be considered evidence of a fact is a fundamental distinction which no legal system can avoid to make. In many legal systems the handwritten signature is an undisputable evidence of the existence of a wilful declaration. In other systems more aspects have to be considered to assess the existence of a wilful act.

These legal differences can thus not be affected by the technical features of the electronic signature: the legal relevance of the electronic signature will only be defined by the specific legal system in which it has been applied.

It should also be noted that an “electronic signature” as defined does not mandate the use of asymmetric cryptography; also symmetric cryptography may be applied. In fact, the definition does not even require the use of cryptography, as long as the stated requirements are fulfilled.

5.3 Advanced Electronic Signature definition

The “advanced electronic signature“ is an electronic signature, which satisfies the four security requirements set out above in the box in section 5.2 Article 2 of the Directive. The requirements are formulated in a technology-neutral way: it is irrelevant by which technological means the security objectives are reached. The definition consequently leaves the door open for future innovation in this domain.

In practice it is however very difficult to work with such a broad and technology-neutral definition. In case of a dispute, a judge, arbitrator or expert would have to verify each time whether the four security requirements are satisfied or not. Because the requirements are formulated in such very general terms, there is much room left for personal judgement, the outcome of which is difficult to anticipate. The present guideline therefore aims to assist in defining the legal consequences of technical differences between electronic signatures in general and advanced electronic signatures.

The technical difference between electronic signatures and advanced electronic signatures has no direct impact on the legal relevance of those signatures. Such technical differences can only have an impact on the way technical evidence is presented to the court, in order to define the precise legal relevance of the signed data.

The criteria to distinguish an advanced signature from an electronic signature are not easy to be deducted following the four requirements provided by article 2.2 of the Directive. Different understandings of article 2.2 are possible. Let us therefore analyze the different requirements of the advanced electronic signature:

a) "Uniquely linked to the signatory": The most commonly used mechanism to realize this today is a X.509 certificate. The possible unique links to the signatory are:

   i) A qualified certificate (X509), which is by definition issued always by a trusted third party

   ii) A non-qualified X509 certificate

      1) issued by a trusted third party

      2) issued by the signatory himself

   iii) Any other kind of electronic attestation complying with the definition set by art. 2.9 of the Directive, i.e. which links signature verification data to a signatory and confirms the identity of that signatory (like conceivable through trusted environments, banking, clearing, telecommunication, ISP services etc)

   The link between the advanced electronic signature and the signatory is created through a reference to the certificate in the signature. The certificate itself may optionally also be attached to the signed document. This allows for verifying the electronic signature, without the need to be on-line and download the Signature Verification Data (SVD) from the Certification Service Provider (CSP).

   While this document is mainly aligned along the public key infrastructure X.509 (PKIX) scope, other certificates than those based on X.509 are conceivable and may serve the provisions of the Directive as well.

b) “Capable of identifying the signatory": This means that it must be possible to identify the signatory from the referred certificate. Without such a technical feature, there will be only an electronic signature (not advanced). Even if the link to the signatory can be evidenced through other means (such as ISP records, an E-Witness, or memorisation of the transaction through the telecommunication provider), it will not be possible to categorize such a signature as an advanced one. However, it is possible to have a link to the signatory using a pseudonym in the certificate, if the CSP holds the personal data identifying the signatory.

c) "Created using means that the signatory can maintain under his sole control": This is a requirement for the access control to the Signature Creation Device (SCDev) containing the signature-creation data (SCD). The access control has to be implemented in such a way that the signatory is able, using a certain procedure, to be sure that his/her SCD and/or SCDev can be utilized only by himself/herself in order to sign data. This means that the signatory may have to be somehow “active” in protecting his/her secret data. (Note: With a Secure Signature-Creation Device (SSCD), as specified in Annex III and required for Qualified Electronic Signatures, no activity is required by the signatory in order to maintain secret his/her SCD. He only has to refrain from disclosing the activation data of his SCD stored in his SSCD.)

Access control for creating advanced electronic signatures thus has to have the following characteristics:

i) If the SCDev is an independent device, having the sole function of signing data, such requirement can apply only to the SCDev.

ii) If the SCDev is a multifunctional device, such as a PC, Laptop, PDA or Mobile Phone, the requirement can apply to the signature-creation application (SCA) and/or to the access to the SCD.

iii) Key backup/recovery can be allowed, with specific procedures to leave it under the sole control of the signatory.

iv) Key escrow can not be allowed, because it excludes per definition the sole control over the SCD.

It should be noted that the requirement for sole control precludes the use of symmetric cryptography, where the secret key is available both to the signer and verifier.

d) "Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable": This leads to requirements for:

i) Signing a true representation of the data. This is normally performed by signing a cryptographic hash of the data. Only hashing functions which meet certain quality metrics can provide a reliable way to detect changes in the signed data. Therefore a Cyclic Redundancy Check (CRC) is for example not an acceptable solution;

ii) Security features:

1) The signing algorithm has to be adequate to the security required (an algorithm with sufficient strength).

2) The key data has to be adequate to the security required. Especially the key length must be secure against brute force and other attacks.

5.4 Qualified Electronic Signature definition

Article 5 of 93/1999/EC

> 1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
>
> (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
>
> (b) are admissible as evidence in legal proceedings.

To avoid technically and legally complex evidence assessment, the European Directive 93/1999/EC introduces a third level of signature in article 5.1, commonly called the “**qualified electronic signature**”. Qualified electronic signatures are advanced electronic signatures, which satisfy specific security requirements listed in the annexes of the Directive. The requirements relate to the content of the certificate on which the electronic signature is based (annex I), the quality of the issuer of that certificate (annex II) and the technical means used to create the signature (annex III).

According to the definition provided by the Directive, a qualified electronic signature is firstly an advanced electronic signature.

Following the definition given (in particular) by article 2.2 of the Directive, and completing it with the requirements provided by Annex I, Annex II and Annex III of the Directive, a qualified electronic signature has the following requirements:

a) The qualified electronic signature must contain a reference to a qualified certificate, issued by a CSP fulfilling Annex II.

b) The qualified electronic signature must be capable to identify the signatory from the referred qualified certificate. If a pseudonym is used, the CSP may be obliged to, pursuant to national law, reveal personal identification data of the holder of the certificate.

c) An SSCD must be used to create the qualified electronic signature. Furthermore, key escrow cannot be allowed, because they exclude per definition the sole control over the SCD.

d) The qualified electronic signature must be linked to the data to which it relates in such a manner that any subsequent change of the data is detectable, as described above.

However, the most relevant differences are of legal nature and are a consequence of the formulation of article 5.1 of the Directive, where not technical means are defined, but functional and security requirements. To rely therefore on a technically based definition of the differences between advanced and qualified electronic signatures could be misleading.

The consequence from a legal perspective can be formulated as follows: **It is the responsibility of the receiver of the signed message to verify that the signature actually is a qualified electronic signature, and thus can be trusted as such.** This can be described as follows (referring to the previous paragraph):

a) The certificate referenced in the signed message must be identified as qualified (using for example the QC extension, or referring to the QC Policy).

b) The supervision scheme shall ensure that the CSP issuing qualified certificates fulfils the requirements laid out by Annex II of the Directive.

c) The technology used to create the signature, the SSCD, must be approved.

d) If the policy “QC + SSCD” is stated in the certificate, the CA has ensured that the SCD is contained in an SSCD. Otherwise, this has to be ensured by the receiver in some other way.

Legal Relevance of Different Types of Electronic Signature

With article 5 of the 93/1999/EC Directive, the European legislator defines the legal relevance of:

- “5.1 signatures", giving them the same relevance as handwritten signatures, requiring the government legislation to ensure that qualified electronic signatures satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data

- "5.2 signatures", stating that these can not be denied legal relevance solely on grounds, as follows:

Article 5 of 93/1999/EC

1. (Stated above)

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

—in electronic form, or

—not based upon a qualified certificate, or

—not based upon a qualified certificate issued by an accredited certification-service-provider, or

---not created by a secure signature-creation device

The great difference between the legal definitions of the two types of electronic signatures in article 5 is that we have a positive definition of a 5.1 signature, and only a residual definition of the other electronic signature: From the legal perspective, a 5.2 signature is every electronic signature which is not a 5.1 signature.

Therefore, it has to be clarified if there is just one type or many types of 5.2 signatures. The answer is clear: there are at least two types of 5.2 signatures, the advanced one and the non-advanced one.

Are there more than theses two types of 5.2 signatures? We have already stated that no difference of legal relevance can be defined separate from a specific legal system. The legal relevance of signatures as such is significantly different in each legal system.

6 Use Cases for Non-Qualified Electronic Signatures

In real life systems designers may wish to build a system that does not contain all the components required by the Directive for a Qualified Electronic Signature, but still use the infrastructure described by the Directive. This chapter discusses electronic signatures which are not qualified electronic signatures, since they are missing some of the elements defined in article 5.1 of the Directive, but still represent valuable use cases.

Many other cases of non qualified electronic signatures are conceivable, but not included in the scope of the present deliverable.

The added value of electronic signatures that make use of some, but not all elements defined for qualified electronic signatures in article 5.1 is also explicitly stated in Directive recital (20) as follows:

Recital (20) of 93/1999/EC

(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; **advanced electronic signatures based on qualified certificates aim at a higher level of security**; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled;

This chapter first describes the use case for Qualified Electronic Signature, and then describes the use cases for electronic signature where one component at a time is missing. First, section 6.2 discusses the use case printed **bold** in the citation of recital (20) given above. Section 6.3 continues with electronic signatures where perceivable document representation is missing. Finally, section 6.4 discusses advanced electronic signatures that use SSCDs but are not based on qualified certificates.

6.1 The Components of Qualified Electronic Signatures

The signature system, as defined in the Directive, has three main components: the Advanced Signature (AS), the Qualified Certificate (QC) and the Secure Signature Creation Device (SSCD). The usage of these components when verifying a signature by a verifier is illustrated by the following figure.

Error! Objects cannot be created from editing field codes.

The AS, the QC and the SCDev link the elements of the certification generation, the creation and the verification of electronic signatures. For concerns of simplicity, we assume that the SCDev implements both the cryptographic mechanisms for the generation of the SCD/SVD pair and for the digital signatures as part of the AS.

The QC contains the name of the signatory or a pseudonym, which shall be identified as such (Annex I c). The identity of the person to which a QC is issued shall be verified by the CSP (Annex II d). The CSP verifies the correspondence of the SVD to be included in the QC with the SCD under control of the signatory (Annex I e). If the CSP receives the SVD from the SSCD the CSP will link the signatory and the SSCD and request the SSCD to provide a proof of correspondence between the SCD and the

SVD. The CSP takes measures against forgery of certificates (Annex II h) and signs the QC with an AS (Annex I h). QCP may define special rules for SSCD usage and SSCD provision service.

The signatory uses a SCA to prepare the data to be signed (DTBS) for the advanced signature (AS) creation. The AS links the DTBS and the AS in such a manner that any subsequent change of the data is detectable (Article 2.2 d). This link shall be established by digital signature mechanism composed of the hash-function and the signing algorithm. Signatory's sole control of the SCD (Article 2.2 c) result in

(a) Asymmetric cryptographic techniques for signature creation with the SCD and for signature verification with the SVD and

(b) Control of the SCD usage.

Note that a message authentication code (MAC) based on symmetric cryptographic mechanisms like ISO 9797 may create an electronic signature but not an advanced electronic signature. The same key is used for MAC generation and MAC verification and cannot be under sole control of the signatory. The control of the SCD usage by the signatory depends on the lifecycle of the SCD and the SSCD implementing the SCD. It will be discussed thoroughly in the next section.

6.2 Advanced Electronic Signature without SSCD

Article 2 (6) of the Directive defines a signature-creation device, which meets the requirements laid down in Annex III as 'secure-signature-creation device'. The preamble of the Directive states in recital (15) that Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures. The Member States determine designated bodies that are in charge of the conformity assessment of secure signature devices with Annex III.

The security of the SCD and the signature-creation depend on the SSCD and the method of its use. The SSCD environment defines the threats to be adverted by the SSCD under the assumptions about TOE usage. The SSCD shall implement all IT security functions which are necessary to ensure the secrecy of the SCD and support security measures to secure the SVD transmission to the CGA and the signature-creation environment.

However, a signature-creation-device (SCDev) used for creating an advanced signature might be not viewed as SSCD in context of Article 5.2 because

a) Although the security may be very high and actually objectively meeting the requirements of Annex III, the security has not been assessed and approved by a designated body, or

b) The SCDev is not able to provide sufficient security measures to meet the requirements of the Annex III.

In the first case, the security of the electronic signature cannot rely on the assurance in the security features of the SCDev given by a security assessment of the designated body. The assurance in the security features of the SCDev might be based on a manufacturer's declaration or might be missing. The signatory repudiating his signature may refer to potential security weaknesses in the SCD lifecycle that makes signature forgery possible. Therefore the security of the SCD and SCDev for non-repudiation of the signatures is difficult to demonstrate. However, the advanced electronic signature may still serve the purpose of origin authentication and data integrity.

The second case addresses a wide area of practical solutions to protect the SCD and the signature-creation process under additional assumptions about the SSCD usage. The crucial assumption is the secure IT environment. Suppose the SCDev is implemented as software for standard personal computers (PCs). The SCDev is then running under the operating system (OS) that provides access to the IT resources like stored data, screen, keyboard and memory by each process. The inactive SCDev is simply a set of data which might be read and manipulated. Therefore, the SCD protection and the self-protection of the SCDev are limited. The SSCD security measures against remaining threats rely substantially on the IT and non-IT environment. The signatory is requested to ensure these security measures. This would be feasible if the SCD, the SCDev and the IT environment is completely under his control. But it is very difficult or impossible to control the IT environment completely, even if the SCDev is running on the signatory's PC. Thus, the signatory must make a compromise between the security needed for his electronic signature and the security measures of the signature environment including the SCDev.

The protection profile in the [SCDEV-PP] document describes one possible approach. This approach may be summarised like this:

(1) The SCDev is under sole control of the signatory. The signatory is the only authorised user of the SCDev including all administrator functions such as installation and initialisation.

(2) The SCDev uses strong cryptographic mechanisms for the generation of the SCD/SVD pair and for the digital signatures.

(3) The SCDev provides user authentication and access control for usage of the generation of the SCD/SVD pair and the signature-creation. The authentication data (password) of the signatory is the only secret not stored electronically.

(4) The SCDev implements elementary measures of self-tests to protect itself against errors and manipulation.

(5) The SCDev relies on protection by the operating system for domain separation. The non-IT environment shall physically protect the SCD, the SCDev and the IT platform.

Let us now look at the use case for advanced signatures without SSCD, as illustrated in the following figure.

Error! Objects cannot be created from editing field codes.

In this use case, a reference to the protection mechanism that enforces the correspondence of the QC to the SCD is now missing. This missing reference requires the verifier to trust the signatory to properly protect the SCD. Although the system in use may provide even greater protection than an SSCD, the Directive specifies that this is not a qualified electronic signature, as the requirements of its Annex III are not fulfilled, or not assessed by a designated body.

This system thus requires the verifier to trust the signatory to properly protect the SCD and only use the SCD appropriately. This system has a potentially weaker link to the person of the signer than the SSCD: since the SCD protection is not strong, the signatory can later claim that the SCD was stolen and used by some other entity.

However, losing the third-party assurance of the SCD protection may not be an issue in some environments; if the verifier can assure through some other means that the SCD was held in a secure location, the verifier can have reliance on the signature as for a normal qualified electronic signature. If the verifier is unable to make this assertion, the verifier does not have the ability to match the SCD with the signatory.

In this use case, the verifier may not be able to get non-repudiation in a court of law, but in a closed environment this may not be necessary. An example of such usage is a system where the SCD is held on a company ID card. The card may not be an assessed SSCD but for use in signing internal documents it is sufficient. If the card usage is tied to some physical security, for example where the card is only used in areas where other protections are in place, this could be even stronger than a SSCD solution.

The technical quality and security of the SCDev have a great relevance in order to define the quality of the evidence. For this reason it is relevant to consider applying a Protection Profile for defining the security requirements of SCDevs. Such a PP, defining minimum requirements to provide integrity and origin authentication of the signed data, has been published in [SCDev-PP] . The PP has been designed with the goal of being possible to realize as a pure software implementation. Other evaluation criteria that may be applied to assure the technical quality of the SCDev are [FIPS 140-2] or [ITSEC].

6.3 Advanced Electronic Signature without Qualified Certificate

In the system illustrated by the figure below, there is no Qualified Certificate binding the signatory's identity to the SCD/SVD pair. Instead, the SVD is made available to the verifier in some other way, for example through a non-qualified certificate or PGP.

Error! Objects cannot be created from editing field codes.

In this case, the system lets the verifier know that the signatory used a SCD from a SSCD to create the signature, but the verifier may not have assured third-party knowledge of who the signatory was. The verifier may also know if the information was properly presented to a signatory. There are several use cases that come from this system model: origin authentication, data integrity, anonymity, direct relation and group signing.

In the origin authentication use case, the SVD is contained in certificate which is still trusted by the verifier, although it is not a qualified certificate. The signature will still have "legal effectiveness and admissibility as evidence in legal proceedings", but it may not have the same legal effect as a hand-written signature.

The data integrity use case is very important, and should not be overlooked. The signature over data that was presented to the signatory and then signed using the SSCD allows the verifier to later determine that the document is still unchanged. When the verifier does not care about who signed the document, just that the document was properly signed, this system works well. However, the verifier can not claim that a certain individual signed the document.

The anonymity use case allows the signer to sign using the SSCD and remain somewhat anonymous, for example by using a pseudonym in the certificate. Certainly the verifier does not have any direct evidence of who the signatory was.

The “direct relation” use case is based on the assumption that the signatory identifies himself, provides a public key and performs a proof-of-possession through a direct contact with the verifier. A typical example of this is a Pretty Good Privacy (PGP) key exchange ceremony.

The verifier can now look at two signed objects and know that the same signatory signed both of them. While the verifier can not legally prove that it was the same signatory, the verifier may have good reason to believe that the same signatory signed both objects, if the verifier knows about the physical protections for the SCD, specifically if a SSCD is used. If the SSCD is under control of a single entity then the verifier can build up a history of information regarding the signatory. This information may allow the verifier to identify the signatory with a high degree of accuracy.

The group signing use case is a final example for corporate use. The SSCD is held inside the corporate safe and taken out under controlled circumstances. When an object is later presented as being signed by the corporation, the verifier may certainly have sufficient information to trust that the signatory was the corporation. The verifier does not know which corporate officer actually created the signature, but the verifier is not interested in who did it, just that the signature was created by the company.

Which of these use cases that actually apply in a specific situation depends on whether the verifier cares about the identity of the signatory, and if he trusts the claimed binding between signatory and SVD (through a non-qualified certificate or PGP

6.4 Digital Signature without Data Representation

In this use case, the system is used to digitally sign and verify binary data, consisting of a random number, a "nonce". Please note that also this digital signature is not an "electronic signature" since it is not related to any data.

In several Member States, signature laws prohibit that SSCDs can be used for other purposes than creating qualified electronic signatures, and in any case, it is regarded as "good practice" to use different keys for qualified electronic signatures on documents and for signing a "nonce". However, the "SCDev used for digitally signing a nonce" may still be contained in the same physical device as the

SSCD, and the SCDev may still be evaluated against the requirements of SSCDs and thus provide a high level of security. But strictly speaking, the SCDev containing the SCD for signing a "nonce" is not an SSCD, and the resulting digital signature is not an electronic signature.

Having said this, the use case is still described for completeness.

Error! Objects cannot be created from editing field codes.

In this use case, the verifier knows that the nonce has not been modified, that the signatory signed the nonce and that the SCD is being properly protected in an SCDev. However, the verifier does not know if the nonce of data has any meaning to the signatory.

In order for the signatory to prevent the verifier from later claiming that the information represents some contract or other information, the signatory must have an unambiguous indication that he is digitally signing a nonce and not a document. This unambiguous indication can either be supplied by the SCA in the format of the signature, or by using a separate key with a corresponding certificate that indicates that the key is only for use in signing blobs. One example of such key usage indicator is the “digitalSignature key usage” in X.509 used for authentication.

Note that using an SCD for other means than signing documents may circumvent the secrecy of the SCD. E.g. if the signature algorithms is vulnerable to chosen plaintext attacks on the SCD, employing such a use case needs to keep that in mind. This may e.g. be provided by ensuring that the nonce is hashed prior to employing the SCD.

A typical use of this system is a scheme for proof of possession or authentication. The nonce to be signed is then simply a random number. When validating the resulting digital signature of the nonce the verifier knows that the signatory had control of the SCDev and authorized the signing of the nonce. This should be sufficient to prove to the verifier that the signatory took part in the signing process; hence the verifier can authenticate the identity contained in the certificate.

An example of this usage would be a company ID card that is a SSCD and also contains a properly created SCDev with SCD and SVD. If an authentication application sends the SCDev a nonce to be signed, a properly signed nonce proves that the signatory has the card in his possession and that he just authorized the use of the SCDev. This provides a very secure authentication of a user.

Additionally, the signatory will have difficulties to later repudiate that he created the signature; what he might repudiate is a possible representation of the data. For this reason, when using the system in this manner, no reliance can be put on the content of the nonce or it’s representation to the signatory. When the certificate contains a key usage indicator that states that the key is only for use in digitally signing nonces, there is no danger of any misuse of that key. 24[0]

7 Evidence for electronic signatures

As described earlier, "electronic signature" is a very broad term, which can serve many purposes.

In case of a dispute over an electronic signature message, one needs to look at all available evidence in order to validate the signature and resolve the dispute. The issues of dispute may for example be that:

- The signer denies having performed the signature at all
- The signer acknowledges having performed the signature, but for a different message

Most of the technical evidence needed for the different types of electronic signatures are the same, and can be found in the signed message and in documents that it refers to, such as certificate, CPS and signature policy, as described in the following sections. However, the following should be noted:

- The signature as declaration of will/intention requires evidence of the context in which the signature was created. This is described in the last section of this chapter.

7.1 Evidence present in the signed data

The signed data will in itself contain the following basic pieces of evidence necessary for establishing the validity of the signature:

- The Signer's Document: The electronic data to which the electronic signature is attached to or logically associated with.
- The Signature: The string of bits resulting from the signature process, using the SSCD or SCDev.
- An indication of the algorithms being used for hashing the document and for signing the hash value.
- An unambiguous reference to the signer’s certificate selected by the signer, e.g. the certificate itself or a reference to it, possibly together with a hash value of the certificate.

The signed data may also contain the following optional evidence:

- An indication that an SSCD has been used when creating the signature. Although not widely used today, this could be achieved for example by an additional signature created by a device-specific key inside the SSCD. A more common case is that the certificate policy referenced in the signer's certificate or other qualifiers in the certificate may indicate if an SSCD has been used.
- A time-stamp applied on the digital signature, issued by a trusted Time-Stamping Authority (TSA), indicating a time before which the signature has been created.
- Certificate path information up to one trusted anchor, as determined by the signature policy.
- Certificate status information that proves that the certificate was valid at the claimed time of signature-creation. It should however be noted that this information still needs to be collected and saved by the verifier when validating the signature after a certain "grace period" in order to ensure that the certificate was not revoked around the time of signature-creation.
- A commitment type, indicating the semantics of the signature. The commitment type can be indicated in the electronic signature either explicitly using a "commitment type indication" in the electronic signature format, or implicitly or explicitly from the semantics of the signed data.
- A location indicator, specifying the claimed location of the signer at the time he or she applied the signature.
- A signer’s time indicator, specifying the claimed time when the signature was applied.

- A role under which the signature is applied.
- A reference to the Signature Policy under which the signature is to be validated (see below)

7.2 Evidence present in the certificate

The certificate issued by the Certification Authority, referenced or contained in the signed message, contains the following additional pieces of evidence:

- an indication if the certificate is issued as a qualified certificate or not (Annex I)
- the identification of the issuer of the certificate, for example the certification-service-provider and the State in which it is established (Annex I);
- a reference to the Certificate Policy and/or Certificate Practice Statement followed by the CA when issuing the certificate;
- the name of the signatory or a pseudonym, which shall be identified as such (Annex I);
- signature-verification data which correspond to signature-creation data under the control of the signatory (Annex I);
- an indication of the beginning and end of the period of validity of the certificate (Annex I);
- an implicit or explicit reference to where certificate status information (certificate revocation list CRL, or online certificate status protocol OCSP) can be found;
- the identity code of the certificate (Annex I);
- the advanced electronic signature of the certification-service-provider issuing it (Annex I);

Optionally, the certificate may also contain:

- limitations on the scope of use of the certificate, if applicable (Annex I);
- limits on the value of transactions for which the certificate can be used, if applicable (Annex I).

7.3 Evidence present in the Certificate Policy and/or CPS

The Certificate Policy and/or CPS published by the CA contain a large amount of information regarding the requirements met and/or the procedures used when issuing the certificate, thus giving evidence of the trustworthiness of the certificate. The most important pieces of evidence relating to the validity of the signature are the following:

- an indication if the certificate is issued as a qualified certificate or not
- description of the procedures for establishing the identity of the certificate holder
- an indication if the CA certifies that the private key (SCD) is stored in an SSCD or not
- description of the security procedures for the CA, for example relating to the protection of the signing key of the CA

7.4 Evidence regarding Certificate Status

When validating a signed message, it is necessary to establish the status of the certificate (revoked or valid) at the time **when the signature was created.** This type of evidence can be provided in two ways:

- The receiver of the signed message checks the status of the certificate (using CRL or OCSP) after receiving the message, and saves this information together with the message (possibly also time-stamped; see also section 7.1 which includes time-stamps as optional evidence). It should be noticed that the receiver may need to get the status information at two different instants of time: one immediately after receiving the signed message, and one after a certain grace period allowing any possible revocation to propagate to the certificate status information service. The receiver is then sure to have access to the relevant status information, in case of a later dispute.

- The CA stores “historical” certificate status information and provides such information on request. A CRL is required to contain such historical information during the validity period of the certificate, but this information may be deleted from the CRL after the expiry of the certificate.

7.5 Evidence present in the Signature Policy

A signature policy is a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid. A given legal/contractual context may recognize a particular signature policy as meeting its requirements. A signature policy may be issued, for example, by a party relying on the electronic signatures and selected by the signer for use with that relying party. Alternatively, a signature policy may be established through an electronic trading association for use amongst its members. Both the signer and verifier use the same signature policy.

A signature policy may be implicit or explicit. The signature policy may be provided as part of the signed document, out of band, or by other means. The signature policy may be explicitly identified or may be implied by the semantics of the data being signed and/or other external data, like a contract being referenced which itself refers to a signature policy, as well as by the signing context. An explicit signature policy for open usage has a globally unique reference, which is bound to an electronic signature by the signer as part of the signature calculation.

The signature policy may include the following:

- rules for certification path construction/verification (including indication of trusted root certificates to be used)

- rules for use of revocation status information (e.g. CRLs or OCSP responses);

- rules for use of timing information, time-marking and/or time stamping;

- signature validation data to be provided by the signer;

- signature validation data to be collected by verifier.

The signature policy may also include:

- the period during which signatures can be performed under that policy,

- a list of recognized commitment types;

- rules for the use of signer roles;

- any constraints on signature algorithms and key lengths;

- other signature policy rules required to meet the objectives of the signature.

7.6 Evidence at the Registration Authority

The minimum elements required by the Annex I of the Directive are not sufficient to provide a clear and unambiguous identification of the holder of the certificate.

The Registration Authority (RA) acting on behalf of the CSP may keep the registration information that was presented at the time of the registration. The name of the signatory contained in the certificate may not always be sufficient to identify unambiguously the signatory.

In such a case, part of the information that was originally presented may (shall, according to some national legislation) unambiguously identify an individual. This is also the case when a pseudonym is being used.

So even the identity of the signer is information that is not necessarily provided by the signature (even not by the qualified electronic signature) and it is necessary to refer to sources of information that are not necessarily contained in the signed data.

7.7 Evidence not available through the signed message

The following "non-technical" evidence is required to establish the context of the signature creation, and thus constitutes necessary evidence for the electronic signature as a declaration of approval through a wilful act:

- The document was signed as a wilful act. Regardless of all technical evidence, the signatory may still have been deceived or forced by violence to sign

- The signatory has read and understood the complete document. Although the technical signature creation environment should enable him to read the complete document, it can never force him to do so. Furthermore, it needs to be established that the document was written in a language understandable to the signer.

Additional evidence that may be required are the following:

- Place of signing. In some contractual situations this is of importance, and may have to be proven.

- Legal system to be applicable for the signed document.

For documents signed by multiple signers, it may also be necessary to establish the order of signing, and if all signers were present at the same place for signing.