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

WORKSHOP AGREEMENT

CWA 14171

<Month> 2001

PROCEDURES FOR ELECTRONIC SIGNATURE VERIFICATION

This CWA is in the process of being published by CEN.

This is an advance copy produced for the participants at the EESSI Open Meeting of 19 June 2001.

Further copies may be purchased from the CEN Members.

This CEN Workshop Agreement can in no way be held as being an official standard as developed by CEN National members

©2001 CEN all rights of exploitation in any form and by any means reserved world-wide for CEN National Members

Ref. No CWA 14171:2001

Contents

1. Scope....6
2. References....7
3. Definitions and abbreviations....8
3.1. Definitions....8
3.2. Abbreviations....10
4. Signature policy and signature validation policy....11
4.1. The need for a Signature policy....11
4.2. The publication of the Signature Policy....11
4.2.1. Using a trusted channel....12
4.2.2. Using trusted Repositories of registered security policies....12
4.2.3. Using a trusted media....12
4.3. The main contents of the Signature Policy....12
4.3.1. Field of application....12
4.3.2. Signature Validation Policy....12
5. Verification processes....14
5.1. Difference between initial and usual verification....14
5.2. The different categories of verification systems....14
5.2.1. Handling specific signature policies....14
5.2.2. Handling dynamically programmable signature policies....14
5.3. The basic inputs to the initial verification process....14
5.4. Outputs from the initial verification process....17
5.4.1. Output status....17
5.4.2. Validation Data....17
5.4.3. Extended forms of validation data....18
5.5. Verification rules to be followed during the verification process....18
5.5.1. Signer Certificate....19
5.5.1.1. Verification of Qualified Signatures....19
5.5.1.2. Verification of Electronic Signatures using Qualified Certificates....19
5.5.1.3. Verification of other electronic signatures....19
5.5.2. Rules for Certification path construction/verification....20
5.5.2.1. Trust Points....20
5.5.2.2. Certification path....20
5.5.3. Rules for the use of Revocation Status information....21
5.5.4. Rules for the use of Time-stamping or Time-marking....21
5.5.4.1. Trust points and Certificate paths....22
5.5.4.2. Time-stamping Authority Names....22
5.5.5. Rules for algorithm constraints and key lengths....22
5.5.6. Rules for the use of signer roles....22
5.5.6.1. Attribute values....22
5.5.6.2. Trust points for Certified Attributes....22
5.5.6.3. Certification path for Certified Attributes....22
5.5.7. Other Signature Policy rules....23
5.6. Inputs to the verification process....23
5.7. Output from the usual verification process....24
6. Signature verification systems....25
6.1. Initial Signature Verification system....25
6.2. Usual Signature Verification system....26
6.2.1. Verification by a human....27
6.2.1.1. Interface to select the electronic signature to be verified....27
6.2.1.2. Interface to present the description of the Signature Policy which is applicable,....27
6.2.1.3. Interface to present the signer's document....27
6.2.1.4. Interface to present the signer information and the output status,....27
6.2.1.5. Interface to obtain the validation data....28
6.2.1.6. User interface requirements....28
6.2.2. Verification by machine....29
6.2.3. Verification by a Third Party....29
7. Examples of different user environments....30
7.1.1. Home environment....30
7.1.2. Office environment....31

7.1.3. Public environment....31
7.1.4. Mobile environment....32
8. Requirements for signature verification systems....33
8.1. Scope....33
8.2. Hardware and software requirements for tamper-evident and tamper-resistant modules....33
8.3. Assumptions concerning installation and verification of signature verification systems....34
8.4. Requirements for signature verification systems and processes....35
8.4.1. Verification process....35
8.4.1.1. Processes with built-in signature policies....35
8.4.1.2. Processes using externally described signature policies....35
8.4.2. Interface to obtain the definition of the Signature Policy....35
8.4.3. Interface to select the electronic signature to be verified....36
8.4.4. Interface to present the applicable Signature Policy....36
8.4.5. Interface to present the signer's document....36
8.4.6. Interface to present the signer information and the output status....36
8.4.7. Interface to ask for an augmented electronic signature....36
9. Conformity assessment....37
10. Legal Aspects....38
10.1. Legal invalidity of a “technically correct” signature....38
10.2. Risks related to certificate revocation....39
10.3. Dispute settlements....39
10.4. Consumer protection....40
10.5. Data protection....41
10.6. Verification of data incorporated by reference....41
11. Multiple Signatures....42
12. Archive system....44
13. Annex A: Annex IV from the Directive....45
14. Annex B. Continental versus Common Law....46
15. Annex C. Time Stamping....48
16. Annex D. How may a verifier really know who the signer is ?....49
16.1. Using previous contacts....49
16.2. Without previous contact....49
17. Annex E. How does root CAs key management affect the publication of the signature policy ?....50

Foreword

Successful implementation of the European Directive 1999/93/EC on a Community framework for electronic signatures 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. Therefore, the ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players: the European Electronic Signature Standardisation Initiative (EESSI).

In July 1999, EESSI delivered its initial recommendations in the EESSI Expert Report. The report contained an overview of the requirements for standards-related activities, as well as a work programme to meet these requirements. A work repartition was drawn up, allocating between CEN/ISSS and ETSI the standardisation activities. The work was carried out by CEN/ISSS in the Electronic Signatures Workshop (WS/E-SIGN) and by ETSI SEC in the ESI WG. The results are documented in a series of CEN Workshop Agreements (CWA) and ETSI standards.

The production of this CEN Workshop Agreement (CWA) was formally agreed at the Kick-Off meeting of the CEN/ISSS Electronic Signatures Workshop (WS/E-SIGN) on 16-17 December 1999, in response to the initial work plan of the European Electronic Signature Standardization Initiative (EESSI).

There are no formal requirements for signature verification specified in the Directive; annex IV (copied in the annex A) only gives recommendations. However, there is a need for a specification for the signature verification procedure, including both the products used for verification, and their management. Signature verification is a process that can be performed in many ways, for example:

- by a natural person, using his workstation and accompanying software to request verification of a received signature,
- by a computer program, using an automated procedure.

The Directive mentions text “displayed to the verifier”, which might be interpreted as verification by a natural person. However, the second case will be much more frequent and useful in electronic commerce, and guidelines are also needed for automated signature verification by computer programs. Also, the term “displayed” should be interpreted in a more general sense as “presented”, since the signed data may be any type of media (text, sound, video etc).

This CWA has been developed through the collaboration of a number of contributing partners in the E-SIGN Workshop, gathering a wide mix of interests, representing different sectors of industry (manufacturers, end-users, service providers, legal experts, academia, accreditation bodies, standardization organisations and national standards bodies) as well as representatives of the national public and European authorities. The present CWA has received the support of representatives of these sectors. A list of company experts who have supported the document's contents may be obtained from the CEN/ISSS Secretariat.

The final review/endorsement round for this CWA was started on 2001-03-15 and was successfully closed at the Workshop's plenary meeting on 2001-04-04. The final text of this CWA was submitted to CEN for publication on 2001-05-09.

There exists a companion document dealing with the procedures for electronic signature generation, as identified in CWA 14170

Introduction

The following are the major parties involved in a business transaction supported by electronic signatures:

- the Signer,
- the Verifier,
- Certification Service Providers,
- the Arbitrator.

The **Signer** is the entity which creates the electronic signature.

The **Verifier** is the entity which verifies the electronic signature, it may be a single entity or multiple entities.

The **Certification Service Providers** (CSPs) are one or more service providers which help to build trust relationships between the signer and verifier. They may be used by the signer and verifier to assist them in performing their tasks.

The **Arbitrator** is an entity able to arbitrate disputes between a signer and a verifier.

The signer must provide at least a basic form of Electronic Signature. This basic form does not protect against all potential threats of the later denying having created the electronic signature (i.e. does not provide non-repudiation). An advantage of this basic form is that it can be created without accessing on-line services. This form is however insufficient to settle disputes in the long term. Additional information needs to be captured soon after the electronic signature has been generated to provide long term verification properties. This is done at the time of initial verification:

> **An initial verification** must be done soon after an electronic signature is generated in order to capture the additional information that will allow to perform usual verifications, e.g. long term verifications.
>
> **Usual verifications** may be done years after the electronic signature was produced. In order to be able to perform a usual verification there should be not need to capture more data than the data that was captured at the time of the initial verification.

However, (for an archive system) more data may need to be captured afterwards if the cryptography that was used at the time of the signature is likely to be broken soon.

This document identifies the security requirements for the various elements of a signature verification system. Beyond the verification process itself, the document identifies the various interfaces, i.e. Application Programmatic Interfaces (APIs) or Man-Machine Interfaces (MMIs) that are needed, in particular :

- to select the signer's document and the electronic signature to be verified,
- to present the signer's document with the right format,
- to get the signer information and the output status after signature verification,
- to get additional data for long term verification; and
- to fetch information from various CSPs.

This document identifies the data that needs to be captured and archived so that it can be later used for arbitration, should a dispute occur between the signer and verifier. The document uses the concept of a signature policy as the basis to verify an electronic signature.

In order to contribute to the interests of the consumers, i.e. consumer confidence and trust in electronic signatures, the signature verification interface should be as easy and error-free as verifying a hand written signature. It should reduce the probability of human errors and be accessible to most users. This document provides recommendations for the use of the interface and guidance on organisational measures to achieve this confidence.

1. Scope

This document specifies the recommended functionality and assurances for electronic signature verification, in the light of the recommendations in Annex IV from the Directive and in the interest of the consumer.

Its primary purpose is to provide guidance on the way to verify qualified electronic signatures that are equivalent to manual signatures according to the chapter 5.1. from the Directive and to explain the importance of the use of time-stamping and/or time marking for the a later verification of the signature.

However, it may also be used when the certificate of the signer is not a Qualified Certificate.

It defines the process to be used and the requirements to be observed by devices for various kind of environments.

2. References

ETSI TS 101 733: Electronic Signature formats
ETSI TS 101 456: Policy requirements for Certification Authorities issuing qualified certificates
ETSI TS 101 862: Qualified Certificate Profile
ETSI TS 101 861: Time Stamping Profile
RFC 2459: PKIX Certificate and CRL Profile
RFC 2560: PKIX Online Certificate Status Protocol
RFC 2559: PKIX Operational Protocols - LDAPv2
RFC 2587: PKIX LDAPv2 Schema

3. Definitions and abbreviations

3.1. Definitions

Certification authority (CA): An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys. [ISO/IEC 9594-8; ITU-T X.509]

Certificate identifier: a unique identifier of a Certificate consisting of the name of the CA and of the certificate serial number assigned by the CA.

Certificate policy: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [ISO/IEC 9594-8; ITU-T X.509].

Certificate validity period: The time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 2459]

Certificate Revocation List: a list containing the serial numbers of revoked certificates from a given CA, together with other revocation information.

Certification path: A chain of multiple certificates, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. [RFC 2459]

Certification-service-provider: an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures; [EC 1999/93]

Commitment Type: a signer-selected indication of the exact intent of an electronic signature - Reference the ETSI Electronic Signature Format Document.

CRL distribution point*:* A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. [ISO/IEC 9594-8; ITU-T X.509]

Data to be signed (DTBS); The complete electronic data to be signed (including both Signer's Document and Signature Attributes)

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 and integrity of the data unit and protect against forgery, e.g. by the recipient (ISO 7498-2).

End entity: A certificate subject which uses its public key for purposes other than signing certificates. [ISO/IEC 9594-8; ITU-T X.509]

Hash function: A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

- It is computationally unfeasible to find for a given output an input which maps to this output
- It is computationally unfeasible to find for a given input a second input which maps to the same output

[ISO/IEC 10118-1]

Initial verification: a process performed by a verifier that must be done soon after a signature is generated in order to capture the information that will make it valid for long term verification.

Object Identifier: a sequence of numbers that uniquely and permanently references an object.

Online Certificate Status Provider: an on line trusted source of certificate status information.

Parallel signatures: the application of separate independent signatures to the same signer's document

Public key: That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1]

Private key: That key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1]

Qualified certificate: a certificate which meets the requirements laid down in Annex I of the Directive and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive; [EC 1999/93]

Qualified electronic signature; an advanced electronic signature which is based on a qualified certificate and which
is created by a secure-signature-creation device (Note: Definition of 5.1 signature taken from the Directive.

Relying party: A user or agent that relies on the data in a certificate in making decisions. [RFC 2459]

Signature attributes: Additional information that is signed together with the Signer's Document.

Signature policy: a set of technical and procedural requirements for the creation and verification of an electronic signature, under which the signature can be determined to be valid.

Signature Policy identifier: Object Identifier that unambiguously identifies a Signature Policy.

Signature policy issuer: An organisation that creates, maintains and publishes a signature policy.

Signature Policy Issuer name: A name of a Signature Policy Issuer.

Signature verification: a process performed by a verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.

Signature-verification-data: data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature; [EC 1999/93]

Signature-verification device: configured software or hardware used to implement the signature-verification-data; [EC 1999/93]

Signer role: the identification of an organisational/operational function that a signer is claiming or allowed to have when invoking the signature process.

Signer's Identity: the registered name of the signer (i.e. as registered by the CSP supplying the signer's certificate).

Signer's Document: The electronic data to which the electronic signature is attached to or logically associated with.

Time-Mark: A proof-of-existence for a datum at a particular point in time, in the form of a record in a secure audit trail, which includes at least a trustworthy time value and a hash representation of the datum.

Time Stamp: A proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.

Time Stamping Authority: An authority trusted by one or more users to provide a Time Stamping Service.

Time Stamping Service: A service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

Usual Verification: a process performed by a verifier that may be done years after the electronic signature was produced, does not need to capture more data than the data that was captured at the time of initial verification.

Validation data: additional data, collected by the signer and/or a verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include: certificates, revocation status information, time-stamps or Time-Marks.

Verifier: an entity that validates or verifies an electronic signature. This may be either a relying party or a third party interested in the validity of an electronic signature.

What Is Presented is What Is Signed (WIPIWIS): a description of the required qualities of the interface able to unambiguously present the signer's document to the verifier according to the content format of the signer's document.

3.2. Abbreviations

CA	Certification Authority
CSP	Certification Service Provider
CP	Certificate Policy
CRL	Certificate Revocation List
ES	Electronic Signature
OID	Object IDentifier
OCSP	Online Certificate Status Protocol
PDA	Personal Digital Assistant
QC	Qualified Certificate
RA	Registration Authority
SCA	Signature Creation Application
SCS	Signature Creation System
SSCD	Secure Signature Creation Device
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSS	Time Stamping Service
WIPIWIS	What Is Presented Is What Is Signed.

4. Signature policy and signature validation policy

4.1. The need for a Signature policy

When two independent parties want to evaluate an electronic signature, it is necessary that they use the same rules in order to get the same result. It is therefore important that the signature policy chosen by the signer must be unambiguously available to the verifying parties. This leads to several requirements:

ą a clear definition of the signature policy SHALL be available to all parties;
ḅ the signature policy applicable to the signed document SHALL be unambiguously recognizable by the verifying parties.

The first condition applies to the Signature Policy Issuers which need to make available the signature policies to the interested parties in a secure manner.

The second condition applies to the signers who need to make sure that no ambiguity is ever possible on the selected signature policy. In any case, the fact that a signature policy is being used SHALL be indicated. However, the reference to a signature policy may be either implicit or explicit.

It is implicit if, from the semantics of the signer's document or more exactly the type of data content being signed, it appears that some *other* documents, like national laws or private contractual agreements, mention that a given signature policy must be used for this type of data content. In this case, a given legal/contractual context may recognize a particular signature policy as meeting its requirements. However, automatic verification outside this context is not possible since, computers cannot determine only from the semantics of the signed data which signature policy shall be used. When the signature policy is implicitly referenced, verification may either automatically take place within a closed context (e.g. where only one type of document is being processed and where the semantics of the document is checked against that type) or may take place with human assistance when it can be proven, using out-of-bands means, which signature policy shall be used with this type of document.

It is explicit, if an explicit reference to the signature policy is indicated by the signer within the electronic signature (and thus protected by the digital signature from the signer). In this case, the benefit is to allow an processing of the electronic signatures, even long after they have been generated and outside their original context of use (e.g. in front of a judge). When the signature policy is explicitly referenced, verification may automatically be performed without any human intelligence/assistance, if the Signature Policy is identifiable by a unique identifier, e.g. an OID (Object Identifier), and verifiable using a hash of the signature policy. In such a case, an electronic signature would include the unique identifier of the signature policy and the hash value of the signature policy and might also include a location (e.g. a URL) where a copy of the Signature Policy may be obtained.

The form and encoding of the specification of the signature policy is not mandated. However, for a given machine processable signature policy, there shall be one and only one definitive form. A signature policy shall be sufficiently definitive to avoid any ambiguity as to its implementation requirements. It SHOULD be absolutely clear under which conditions an electronic signature should be accepted.

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.

4.2. The publication of the Signature Policy

Before signing, a signer SHOULD be sure which security policy will apply. In the same way, when verifying an electronic signature, a verifier needs to make sure to use the right security policy. The security service able to provide that assurance is a combination of two basic security services: data origin authentication service and an integrity service. There are various ways to fulfil these two services in combination and this document does not mandate a particular way as long as the service is offered. However, it is recommended to support one of the three following ways that allow to make sure that the signature policy is genuine.

4.3. Using a trusted channel

Signature Policy Issuers may make available their policies either by placing them on a secure web site (e.g. using TLS / SSL) or by signing them. This is applicable for signers to generate the electronic signature and verifiers to verify the electronic signature soon after it has been generated, but may not be practical for long term verification, because it may not be easy to verify the digital signature of the issuer in the long term, hence other methods are necessary.

4.3.1. Using trusted Repositories of registered security policies

Signature Policy Issuers may disappear and situations where they cannot provide anymore a trusted copy of the policies they have issued may appear. It thus becomes necessary to rely on a third party. For long term verification of Electronic Signatures the use of trusted Repositories of registered Signature Policies is thus needed (e.g. established by the ICC). In that case, it becomes sufficient to connect to these Repositories and access them using a data origin authentication service combined with an integrity service. This may be achieved using TLS (Transport Layer Security). Signature Policies must be kept in Trusted Repositories as long as there is a need to verify an electronic signature that has been made against these Signature Policies.

4.3.2. Using a trusted media

Each Signature Policy Issuer may provide a trusted media to the users, e.g. in the form of a CD-ROM, that can be authenticated as issued by the Signature Policy Issuer.

4.4. The main contents of the Signature Policy

A signature policy MUST include:

- a unique identifier or unambiguous identification of the signature policy;
- the signature policy issuer name;
- the issuing date of the signature policy;
- the **field of application** of the signature policy;
- a **signature validation policy**.

4.4.1. Field of application

The **field of application** of the signature policy is a description of the expected application of this policy and the conditions that apply to the electronic signature. This part of the signature policy can be assessed to meet the requirements of the legal and contractual context in which it is being applied. It is intended to be available for display (or listening) both by the signer or the verifier. This part of the signature policy is similar to the contractual terms that may be found on the back of a contract that apply to all the commitments made under that signature policy.

4.4.2. Signature Validation Policy

The **signature validation policy** specifies the technical rules to be followed by the signer and the verifiers used to process the electronic signature. This rules allow for the initial and usual verifications of electronic signatures issued under that form of signature policy. They may be either described as free text or be described in a machine processable language.

The Signature Validation Policy includes rules defining the components of the electronic signature that SHALL be provided by the signer with data required by the verifier to provide long term proof, as well as rules regarding use of TSPs (CA, OCSP servers, Attribute Authorities, Time Stamping Authorities). For that reason it SHALL include:

- rules for Certification path construction/verification;
- 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.

It should 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.

The signature validation policy may recognize one or more types of commitment as being supported by electronic signatures produced under the security policy.

If an electronic signature does not contain a recognized commitment type then the semantics of the electronic signature is dependent on the data being signed and the context in which it is being used.

5. Verification processes

5.1. Difference between initial and usual verification

The term **verification** is used where an electronic signature is determined to be valid or not. Two specific instances of verifications are specified in this document:

Initial verification that must be done soon after an electronic signature is generated in order to capture the additional information that will make it valid for long term verification.

Usual Verification that may be done years after the electronic signature was produced, does not need to capture more data than the data that was captured at the time of initial verification.

However there is one exception: if the cryptography that was used years before is likely to be broken soon, at that stage more information needs to be gathered in order to extend the life-time of the cryptography.

5.2. The different categories of verification systems

Verification of an electronic signature against a signature policy requires a signature verification system able to process the signature policy. There may be some cases where specific parameters from the security policy (e.g. root keys) are downloaded into the system. In such a case the source of the download SHALL be authenticated and the integrity of the downloaded data SHALL be verified. There are basically two categories of verification systems.

5.2.1. Handling specific signature policies

These systems only support **specific signature policies**. The verification process implemented by the system SHALL conform to a human readable description provided all the processing rules of the signature policy are clearly defined. However, if additional policies need to be supported, then such an implementation would generally need to be customized for each additional policy. This type of implementation may be simpler to implement initially, but can be difficult to enhance to support numerous additional signature policies.

Each verification system must be evaluated against each security policy that is claimed to be supported by the system.

5.2.2. Handling dynamically programmable signature policies

These systems are **dynamically programmable** and able to adapt their rules in accordance with a description of the signature policy provided in a computer-processable language (e.g. ASN.1). This type of implementation is able to support multiple signature policies without being modified every time, provided all the verification rules specified as part of the signature policy are known by the implementation (i.e. only requires modification if there are additional rules specified).

Verification systems must be evaluated once against the security policy descriptive language.

5.3. The basic inputs to the initial verification process

At the time of initial verification a verifier SHALL first unambiguously identify the signature policy that must be used either because it has been explicitly referenced by the signer in the electronic signature or implicitly referenced by the type of data being signed. He SHALL then obtain a copy of the signature policy in a trusted way and make sure that what he gets matches the intended signature policy.

> When an explicit reference is being used, the verifier SHALL make sure that he accesses a trusted copy of the signature policy. He SHALL also evaluate if the signature policy matches his needs either by looking at the details of the signature policy or by making sure that the identifier of the signature policy is acceptable.

When an implicit reference is being used, the verifier needs to understand the semantics of the user data and then SHALL refer to some other trusted documents (e.g. private agreements applicable in some sectors to some kind of transactions) explicitly saying that this type of data, unless otherwise explicitly indicated, is always implicitly referencing a given signature policy.

Initial verification of an electronic signature then requires, on one side a system able to process the signature policy either explicitly referenced by the electronic signature or implicitly referenced by the signer's document and on the other side:

- the signer’s document;
- the electronic signature over the signer’s document;
- any other additional data associated with the electronic signature, called validation data;

Signer’s document is the document that is signed by the signer.

The digital signature SHALL be applied over the following elements :

- the Signer’s Document or hash of it (i.e. a document digest),

- an unambiguous reference to the signer’s certificate selected by the signer, e.g. the certificate itself or a reference to it together with a hash value of the certificate. This is particularly important when a signer holds a number of different certificates that relate to the same signature creation data, to avoid claims by a verifier that another certificate with different semantics is implied by the signature, and also when the signer holds different certificates related to different signature creation data in order to provide the verifier with the correct signature verification data. This is also important in case the issuing key of the CA providing the certificate would be compromised.

In addition, the digital signature shall conditionally cover the following information:

- a Content Format that identifies the format of the signer's document (when electronic signatures are not exchanged in a restricted context) to enable the verifier to be presented or use the signer's document (text, sound or video) in exactly the same way as intended by the signer,

- an identification that a specific Signature Policy is to be used (when electronic signatures are not exchanged in a restricted context and an implicit Signature Policy is being used). In this case, the signature policy must be derived from the semantics of the signer's document or more exactly the type of data content being signed, and some other information, e.g. national laws or private contractual agreements, that mention that a given signature policy must be used for this type of data content. This will ensure that the verifier will be able to use the same signature policy during the verification process. A signature policy is needed to clarify the precise role and commitments that the signer intends to assume with respect to the Signer’s Document, and to avoid claims by the verifier that a different signature policy was implied by the signer,

- an unambiguous reference to a Signature Policy, e.g. the signature policy itself or a reference to it together with a hash value of the signature policy (when an explicit Signature Policy is being used). This will ensure that the verifier is able to use the same signature policy during the verification process. A signature policy is needed to clarify the precise role and commitments that the signer intends to assume with respect to the Signer’s Document, and to avoid claims by the verifier that a different signature policy was implied by the signer,

- a Commitment Type undertaken by the signer in signing the Signer’s Document in the context of the selected signature policy (when an explicit commitment is being used); This will be required where a Signature Policy specifies more than a single Commitment Type, each of which might have different legal interpretations of the intent of the signature (e.g. Proof of Origin, Proof of Receipt, Proof of Creation …);

- any additional information which must be signed to conform with the signature policy.

In addition the digital signature shall cover the following optional information, if present:

- the signing time, as claimed by the signer;
- a content time stamp (to prove that the electronic signature was performed after that time);
- the claimed or certified role(s) assumed by the signer in creating the signature;
- the location of the signer, as claimed by the signer, at which the signature was created.

When verifying an electronic signature it is fundamental to determine unambiguously whether the signer's certificate and the attribute certificates, if any, were *valid at the time the signature was generated*.

This means that in any case an electronic signature SHALL be placed in a time scale.

For an initial verification, when no particular additional information is present to be able to place the signature in a time scale, then the current time is assumed to be very close to the time the signature was generated. So the revocation conditions that apply at the verification time are used. Since they will be more stringent than those applying at the time the signature was generated, there is no risk to accept an invalid electronic signature, but a risk to reject a signature that would have been valid, if verified sooner.

For usual verification, additional information MUST be present, so that it may be proven that the signature was generated while the certificate was valid. This may be achieved in two ways:

ą either using a **Time Stamp** from a Time Stamping Authority (TSA), or
ę using a secure audit trail, where are recorded, at the minimum, both a **Time Mark** and the value of the electronic signature.

The first case has several advantages: it allows to prove the time that the signature was generated before the time indicated in the time stamp without revealing any other information; it only uses digital information that can be copied from one media to another without losing any of the initial properties.

The second case mandates to disclose the format of the audit trail, the procedures uses to create the audit trail and to produce the physical media used to support the audit trail at the time it was recorded and to reveal the other records that are in the audit trail. It would be impossible to standardize the format of such audit trails as well as the use of some physical media adequate for such a recording. In addition, the Trusted Service Provider SHOULD be independent from the plaintiffs, otherwise there might be a collusion between one of the plaintiffs and the Trusted Service Provider. For all these reasons, the use of time stamps, although not mandatory, is highly recommended.

The validation data is the additional data needed to validate the electronic signature; this includes:

* certificates;
* revocation status information (e.g. CRLs and/or OCSP responses),
* trusted time-stamps from Time Stamping Authorities (TSAs) or Time-Marks from Trusted Service Providers.

An electronic signature may exist in many forms including:

* an Electronic Signature (ES), which includes the digital signature and other basic information provided by the signer. The ES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures. It provides basic authentication and integrity protection and can be created without accessing on-line (time stamping) services. However, without the ability to position the electronic signature in a time scale, the digital signature does not protect against the threat that the signer later denies having created the electronic signature at a time the corresponding certificate was valid and not revoked (i.e. it does not provide non-repudiation);

* an ES with Time (ES-T), which either adds a **Time Stamp** from a Time Stamping Authority to the Electronic Signature, to take initial steps towards providing long term validity, or adds a **Time Mark** to the Electronic Signature, by copying both the Electronic Signature and the Time Mark in a secure audit trail;

- an ES with Complete validation data (ES-C), which adds to the ES-T the references to (but not the values of) the complete set of data supporting the validity of the electronic signature (e.g. certification path and revocation status information). The ES-C thus contains both the references of the validation data *and their hash values.* This allows to make sure that the actual values which has been captured are the one's referenced. The complete set of data supporting the validity of the electronic signature does not necessarily need to be kept together with the Electronic Signature but may be kept somewhere else. The ES-C is the common denominator of two other forms of ES. One form (identical to the ES-C) allows to store these values elsewhere, e.g. in some central storage, while the other form (ES-X) allows to store all the values of the validation data together with the ES.

The signer SHALL provide at least the ES form.

5.4. Outputs from the initial verification process

The **initial verification Process** validates an electronic signature in accordance with the requirements of the signature policy. There are two outputs: an output status and output data, called validation data.

5.4.1. Output status

The output status of the initial verification process can be:

- passed verification;
- failed verification;
- incomplete verification.

A **Passed Verification** response indicates that the signature has passed verification and it complies with the signature validation policy.

An **Failed Verification** response indicates that the signature does not comply with the signature validation policy, e.g. the format is incorrect, the digital signature value failed verification or the signer’s certificate has been revoked.

An **Incomplete Verification** response indicates that the format and digital signature verifications have not failed but there is insufficient information to determine if the electronic signature is valid under the signature policy. It may be possible to request that the electronic signature be checked again at a later date when additional validation information might become available. Also, in the case of Incomplete verification, additional information may be made available to the application or user, thus allowing the application or user to decide what to do with partially correct electronic signatures.

5.4.2. Validation Data

The **Validation Data** SHALL be collected by the verifier and SHALL meet all the requirements of the signature policy.

Basically, if there may be a need for a subsequent usual verification, the validation data SHALL contain the proof that the certification path that was used was valid *at the time the signature was generated*.

This means that a full certification path and the associated revocation status information for each certificate from the path SHALL be captured. The validation data includes CA certificates as well as revocation status information in the form of certificate revocation lists (CRLs) or certificate status information provided by an on-line service.

In order to prove that that the data was captured before revocation occurred or before the end of the validity period of the certificate, and if there is a need for a subsequent usual verification a time stamp over the electronic signature or a secure audit trail SHALL be used to provide evidence of the timing of given events. It may be required, as a minimum, that either the signer or verifier obtains a time stamp over the signer's signature.

The signer may decide, in some cases, to provide more data than the ES form and in the extreme case could provide an electronic signature with complete validation data (e.g. the ES-C form). The **Validation Data** *may* thus also be collected by the signer and fully provided to the verifier.

When if there is a need for a subsequent usual verification, if the signer does not provide ES-T, the verifier SHALL create the ES-T on first receipt of an electronic signature. The ES-T provides independent evidence of the existence of the signature at the time it was first verified which should be near the time it was created, and so protects against later repudiation of the existence of the signature. If the signer does not provide ES-C the verifier SHALL create the ES-C when the complete set of revocation and other validation data is still available.

The ES-T time-stamp should be created close to the time that ES was created to provide maximum protection against repudiation. At this time all the data needed to complete the verification may not yet be available but what information is readily available may be used to carry out some of the initial checks. For example, only part of the revocation information may be available for verification at that point in time.

Generally, the ES-C form cannot be created at the same time as the ES, as it is necessary to allow time for any revocation information to be reported by the real signer. Also, if a certificate is found to be temporarily suspended, it will be necessary to wait until the end of the suspension period.

5.4.3. Extended forms of validation data

The complete validation data (ES-C) described above may be extended to form an ES with eXtended validation data (ES-X) to allow the storage all the values of the validation data together with the ES in particular:

- the signer's certificate,
- all the CA certificates that make up the full certification path, as referenced in the ES-C,
- all the associated revocation status information, as referenced in the ES-C.

then the values of these elements may be added to the ES-C. This form of extended validation data is called ES-X.
Alternatively, it is possible to keep at least the signer's certificate in the ES-X and store CAs certificates and CRLs in some central place. This is more efficient in terms of storage when electronic signatures are received from subjects certified by the same CAs.

A verifier may be required to provide on request, proof that the certification path and the revocation information used a the time of the signature were valid, even in the case where one of the issuing keys or OCSP responder keys is later compromised. Additional information in the validation data is able to provide such a protection.

Before the algorithms, keys and other cryptographic data used at the time the validation data was constructed become weak and the cryptographic functions become vulnerable, or the certificates supporting previous time stamps expires, the signed data, the validation data should be time stamped using stronger algorithms (or longer key lengths) than in the original time stamp.

The Time stamping process may be repeated every time the protection used to time stamp a previous validation data becomes weak. Validation data may thus include multiple embedded time stamps.

5.5. Verification rules to be followed during the verification process

By specifying the requirements on the signer and verifier the responsibilities of the two parties can be clearly defined to establish all the necessary information.

An electronic signature SHALL be valid when:

- It contains a minimum set of elements so that initial verification can take place;
- Suitable validation data is available, e.g. additional certificates, CRLs, results of on line certificate status checks and to use time stamps (if not already provided by the signer) or time-marks,
- The verification is performed by a trusted verification system.

5.5.1. Signer Certificate

5.5.1.1.Verification of Qualified Signatures

For the verification of Qualified Signatures, the signer certificate SHALL be a Qualified Certificate where the use of an SSCD is required.

When using an Internet X.509 Public Key Infrastructure, the indication that a certificate is issued as a Qualified Certificate is provided when one of the certificate policies identified in the Certificate Policies extensions, as defined in section 4.2.1.5 from RFC 2459, clearly express that the issuer intentionally has issued the certificate as a Qualified Certificate and that the issuer claims compliance with Annex I and Annex II of the Directive. In such a case, the identifier for the qualified certificate policy will be " **QCP public + SSCD"** (A certificate policy identifier for qualified certificates issued to the public, requiring use of secure signature-creation devices). The OID is: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)

For signatures complying with article 5.1, the key usage extension of the signer certificate SHALL be present and the non repudiation bit (NR bit) SHALL be set. The digital signature bit (DS bit) should not be set as indicated in section 3.2.3 from the Qualified Certificates Profile.

5.5.1.2. Verification of Electronic Signatures using Qualified Certificates

For the verification of Electronic Signatures using Qualified Certificates, the signer certificate SHALL be a Qualified Certificate where the use of an SSCD is not required.

When using an Internet X.509 Public Key Infrastructure, the indication that a certificate is issued as a Qualified Certificate is provided either:

1. when one of the certificate policies identified in the Certificate Policies extensions, as defined in section 4.2.1.5 from RFC 2459, clearly express that the issuer intentionally has issued the certificate as a Qualified Certificate and that the issuer claims compliance with Annex I and Annex II of the Directive. In such a case, the identifier for the qualified certificate policy will be "**QCP public".** (A certificate policy for qualified certificates issued to the public, not requiring the use of secure signature creation devices). The OID is: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public (2), or

2. when the Qualified Certificate Statements extension includes a statement, to express it . In that case, an individual statement placed in a QCStatements extension indicates that "the certificate is issued as a Qualified certificate according Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the country specified in the issuer field of this certificate". The OID is: itu-t(0) identified-organization(4) etsi(0)
   id-qc-profile(1862) id-qc-profile(1862) qc-statements(1) QcCompliance(1).

Note: combination of both techniques is not necessary, but permitted.

5.5.1.3.Verification of other electronic signatures

For the verification of other electronic signatures that would exhibit the same properties with the single exception that the certificate from the signer is not a Qualified Certificate, then there is no requirement for the signer's certificate to be a Qualified Certificate. The key usage extension of the signer certificate SHALL be present and the non repudiation bit (NR bit) SHALL be set. The digital signature bit (DS bit) should not be set.

5.5.2. Rules for Certification path construction/verification

The certificates that may be used by the signer to provide a valid electronic signature, may be constrained by the combination of the trust point and certificate path constraints in the signature validation policy.

5.5.2.1.Trust Points

The signature validation policy defines the certification authority trust points that are to be used for signature verification. Several trust points may be specified under one signature policy. Specific trust points (i.e. root certificates with additional data) may be specified for a particular type of explicit or implicit commitment defined under the signature policy. If one of the trust points is changed, then the a new version of the signature policy has to be issued. For a signature to be valid a certification path SHALL exists between the Certification Authority that has granted the certificate selected by the signer (i.e. the used user-certificate) and one of the trust points of the Signature Validation Policy.

5.5.2.2.Certification path

For an electronic signature to be valid, any constraints on the use of certificates in the certification path SHALL be honoured, i.e. the content of the signer certificate and the certificates issued by one or more CA(s) in the certificate chain and trust points. The two prime constraints are certificate policy constraints and naming constraints:

- Certificate policy constraints limit the certification chain between the user certificate and the certificate of the trusted point to a given set of certificate policies, or equivalents identified through certificate policy mapping. Mandating the use of some Certificate Policies for the certificate from the signer, may mean that the signer has agreed to use an adequate level of protection of the private signature key and/or that he has agreed to use a secure creation environment, e.g. the use of a Secure Signature Creation Environment (SSCE) in conjunction with a Secure Signature Creation Device (SSCD).

- The naming constraints limit the forms of names that the CA is allowed to certify.

Naming constraints are particularly important when a "Signature policy" identifies more than one trust point. In this case, a certificate of a particular trusted point may only be used to verify signatures from users with names permitted under the name constraint.

Certificate Authorities may be organized in a tree structure, this tree structure may represent the trust relationship between various CA(s) and the users CA. Alternatively, a mesh relationship may exist where a combination of tree and peer cross-certificates may be used. The certificate path provides the trust relationship between the trusted CAs and the signer’s user certificate. The starting point from a verification point of view, is the "trust point". A trust point is usually a CA that publishes self-signed certificates, it is the starting point from which the verifier verifies the certificate chain. Naming constraints may apply from the trust point, in which case they apply throughout the set of certificates that make up the certificate path down to the signer's user certificate.

Certificate Policy constraints can be easier to process but to be effective require the presence of a certificate policy identifier in the certificates used in a certification path.

However, all certificate policy constrains and all naming constraints cannot always be placed in self-signed certificates. The syntax would be too complex and such certificates would be overloaded. For that reason, it is easier to express policy constraints and naming constraints in the security validation policy, but outside the self signed certificates.

Certificate path processing, thus generally starts with one of the trust points from the signature policy and ends with the user certificate.

When using an Internet X.509 Public Key Infrastructure, the certificate path processing procedures defined in RFC 2459 clause 6 (or its successor) defines the *mandatory* conditions for a path to be valid. Other additional conditions may apply and thus this verification while *mandatory* is not *sufficient* to accept a certificate as valid.

The signature validation policy identifies the following initial parameters that are selected by the verifier in certificate path processing:

- acceptable certificate policies;
- naming constraints in terms of constrained and excluded naming subtrees;
- requirements for explicit certificate policy indication and whether certificate policy mapping are allowed;
- restrictions on the certificate path length.

The signature validation policy identifies additional constraints on these parameters.

5.5.3. Rules for the use of Revocation Status information

The signature policy should define rules specifying requirements for the use of certificate revocation lists (CRLs) and/or on-line certificate status check service (e.g. using OCSP) to check the validity of a certificate. These rules specify the mandated minimum checks that SHALL be carried out.

The verifier may take into account information in the certificate in deciding how best to obtain and check the revocation status (e.g. a certificate extension field about authority information access or a CRL distribution point) provided that it is also in accordance with the signature policy revocation rules.

Before an electronic signature may really be valid, the verifier has to be sure that the legitimate holder of the private signature key was really the only one in possession of key at the time of signing. However, there is an inevitable delay between a compromise or loss of key being noted, and a report of revocation being distributed. To allow greater confidence in the validity of a signature, a "cautionary period" may be identified in the signature validation policy before an electronic signature may be said to be valid. A verifier may need to wait until the end of that period before fetching the revocation status information. The verification policy may specify such a cautionary period.

Note: The verifier care has to take special attention to the following situation:

1. At a claimed “time 1” the signer applies the electronic signature to the document to be signed.
2. The electronic signature is Time Stamped or Time Marked at time 2, later than time 1.
3. The cautionary period is added to time 2 and thus ends at “time 3”.
4. The certificate is revoked at “time 4” which may be earlier or later than time 3.
5. The electronic signature is initially verified at “time 5”, which may not be earlier than time 3.

If the certificate is revoked before time 3, then the electronic signature fails verification.
If the certificate is revoked after time 3, then the electronic signature passes verification.

In case that there is no proof for the verifier that the electronic signature was time stamped or time marked, then the electronic signature must not pass verification successfully.

5.5.4. Rules for the use of Time-stamping or Time-marking

When time marking is being used, the ES SHALL be recorded in a secure audit trail.

When time stamping is being used, the following rules should be followed when specifying, constraints on the certificate paths for time-stamping authorities, constraints on the time-stamping authority names and general timing constraints. There will be some delay between the time that a signature is created and the time the signer's signature is time-stamped. However, the longer this elapsed period the greater the risk of the signature being invalidated due to compromise or deliberate revocation of its private signing key by the signer. Thus the signature policy should specify a maximum acceptable delay between the signing time as claimed by the signer and the time included within the time-stamp. If no delay is specified, then, at latest, the electronic signature SHALL be time-stamped or time-marked at the very end of the validity period of the certificate (because the CA will not accept any new declaration of private key compromises beyond the end of the validity period).

5.5.4.1.Trust points and Certificate paths

Signature keys from time-stamping authorities will need to be supported by a certification path. The certification path used for time-stamping authorities requires a trust point and possibly path constraints in the same way that the certificate path for the signer's key.

5.5.4.2.Time-stamping Authority Names

Restrictions may need to be placed by the validation policy on the named entities that may act a time-stamping authorities.

5.5.5. Rules for algorithm constraints and key lengths

The signature validation policy may identify a set of signing algorithms (hashing, public key, combinations) and minimum key lengths that may be used:

- by the signer when creating the signature;
- in end entity public key Certificates;
- CA Certificates;
- attribute Certificates;
- by the Time Stamping Authority.

5.5.6. Rules for the use of signer roles

Roles are optional and can be supported as claimed signer roles or as certified signer roles using Attribute Certificates.

5.5.6.1.Attribute values

When signature under a signer role is mandated by the signature policy, then either Attribute Certificates may be used or the signer may provide a claimed signer role attribute. The acceptable attribute types or values may be dependent on the type of commitment. For example, a user may have several signer roles that allow the user to sign data that imply commitments based on one or more of his roles.

For machine processable verification of attributes, it is crucial that the signer roles are encoded in an unambiguous manner.

5.5.6.2.Trust points for Certified Attributes

When a signature under a certified role is mandated by the signature policy, Attribute Authorities are used and need to be validated as part of the overall verification of the electronic signature. The trust points for Attribute Authorities do not need to be the same as the trust points to evaluate a certificate from the CA of the signer. Thus the trust point for verifying roles need not be the same as trust point used to validate the certificate path of the user’s key.

Naming and certification policy constraints may apply to the AA in similar circumstance to when they apply to CA. Constraints on the AA and CA need not be exactly the same. AA(s) may be used when a signer is creating a signature on behalf of an organization, they can be particularly useful when the signature represents an organizational role. AA(s) may or may not be the same authority as CA(s).

Thus, the Signature Policy identifies trust points that can be used for Attribute Authorities (AAs), either by reference to the same trust points as used for Certification Authorities, or by an independent list.

5.5.6.3.Certification path for Certified Attributes

Attribute Authorities may be organized in a tree structure in similar way to CA where the AAs are the leafs of such a tree. Naming and other constraints may be required on attribute certificate paths in a similar manner to other electronic signature certificate paths.

Thus, the Signature Policy may identify additional constraints on the following parameters used as input to the certificate path processing:

- acceptable certificate policies, including requirements for explicit certificate policy indication and whether certificate policy mapping is allowed;
- naming constraints in terms of constrained and excluded naming sub-trees;
- restrictions on the certificate path length.

5.5.7. Other Signature Policy rules

The signature policy may specify additional policy rules, for example rules that relate to the environment used by the signer. These additional rules may be defined in computer processable and/or human readable form.

5.6. Inputs to the verification process

At the time of verification, which may be years after the electronic signature was done, a verifier must unambiguously identify the signature policy that SHALL be used. This can be obtained either because the signature policy has been explicitly referenced by the signer in the electronic signature or because the signature policy is been implicitly referenced by the type of data being signed. He SHALL then obtain a copy of the signature policy in a trusted way and make sure that what he gets matches the intended signature policy.

When an explicit reference is being used, he shall use the OID of the policy and make sure that he obtains a trusted copy of the signature policy. This may be done using a hash of the signature policy that has been computed by the signer. In such a case, the verifier SHALL first compute the hash value over the trusted copy of the signature policy he has just obtained and make sure it matches the hash originally computed by the signer.He SHALL also make sure that the identifier of the signature policy is acceptable.

When an implicit reference is being used, the verifier needs to understand the semantics of the user data and then SHALL refer to some other trusted documents (e.g. private agreements applicable in some sectors to some kind of transactions) explicitly saying that this type of data, unless otherwise explicitly indicated, is always implicitly referencing a given signature policy.

In any case, he SHALL also evaluate if the signature policy matches his needs by looking at the details of the signature policy (this only needs to be done once).

Verification of an electronic signature then requires, on one side a system able to process the signature policy either explicitly referenced by the electronic signature or implicitly referenced by the signer's document and on the other side:

- the signer's document;
- the electronic signature over the signer's document;
- any other additional data associated with the electronic signature, i.e. validation data;

The same controls, already described for the initial verification phase occurs, except that all the validation data must be provided by the plaintiff. In particular, it is fundamental to determine unambiguously whether the signer's certificate and the attribute certificates, if any, were *valid at the time the signature was generated*.

This means to present either :

a) a **Time Stamp** over the ES from a Time Stamping Authority (TSA), or
b) an **Secure Audit Trail**, e.g. from an independent Trusted Service Provider [1], that contains both a **Time Mark** and the value of the Electronic Signature.

[1] The Trusted Service Provider should preferably be independent from the parties (plaintiffs and defendants) , otherwise it might be accused to have a collusion with one of the parties.

The first case has several advantages: it allows to prove the time before the signature was generated without revealing any other information; it only uses digital information that can be copied from one media to another without loosing any of the initial properties. However, there is no information about when the signature was generated. The way to solve this issue, is the following: the purported date and time of the signature, as claimed by the signer, can be included in the signed data. For a signed document to be valid under the signature policy, it may be need to be time-stamped by a TSA where the date of the signature as claimed by the signer (if present) and the date of time stamping indicated by the TSA will have to be "close enough". "Close enough" means a few minutes, hours or even days according to the Signature Validation Policy.

The second case mandates to reveal the format of the audit trail, the procedures used to create the audit trail and to produce the physical media and to reveal the other records that are in the audit trail. It would be impossible to standardize the format of such audit trails as well as the use of some physical media adequate for such a recording. For all these reasons, the use of time stamps, although not mandatory, is highly recommended.

5.7. Output from the usual verification process

The **usual verification process** verifies an electronic signature in accordance with the requirements of the signature policy. There is single output status (and no other output data). The output status of the usual verification process is either :

- passed verification, or;
- failed verification;

A **Passed verification** response indicates that the signature has passed verification and it complies with the signature validation policy.

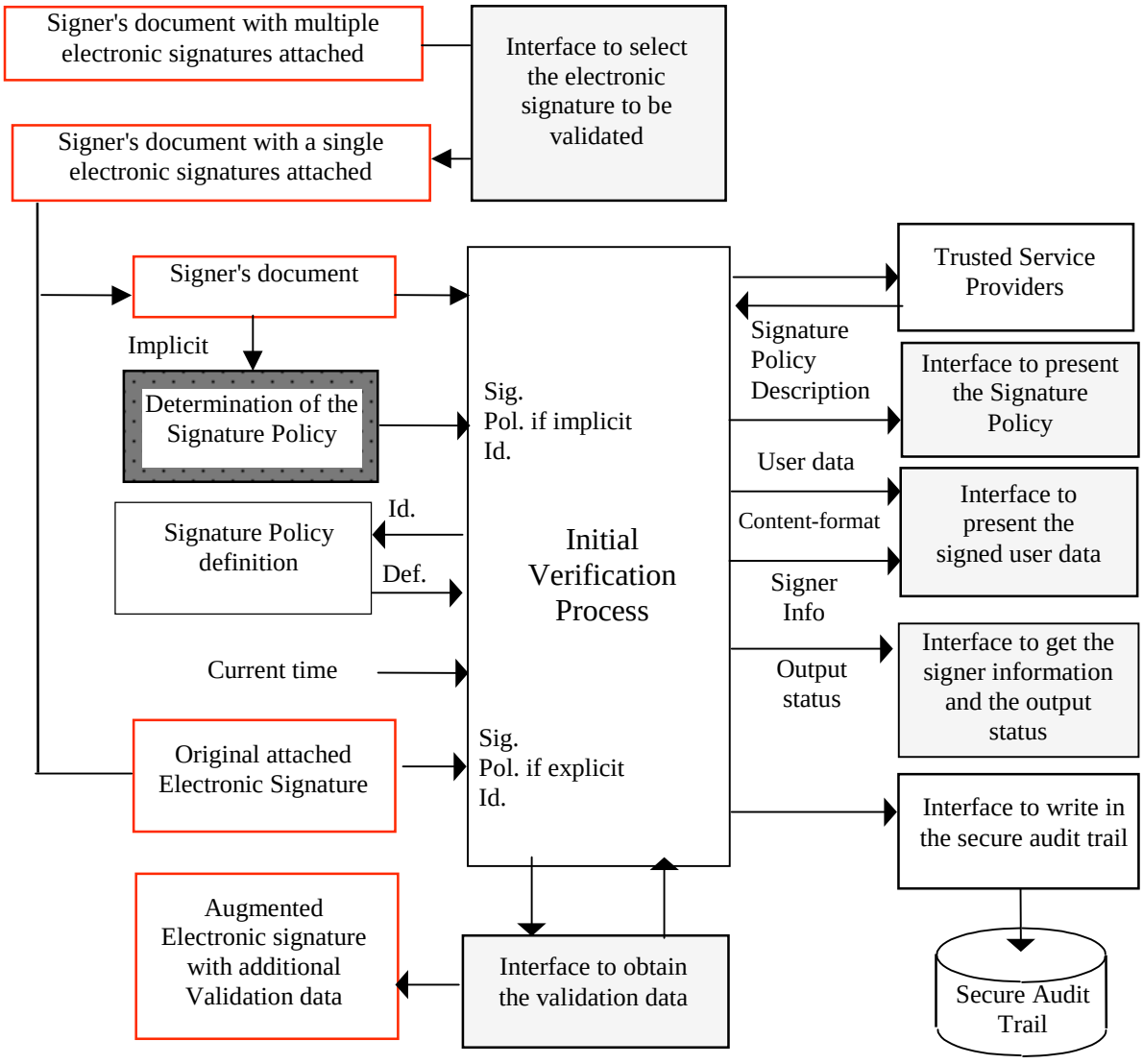
A **Failed Verification** response indicates that the electronic signature fails to comply with the signature validation policy.

6. Signature verification systems

6.1. Initial Signature Verification system

An initial signature verification system is composed of :

- the secure signature verification process,
- an interface to enter the signer's document and to select the electronic signature to be verified (there may be more than one electronic signature attached with the user data),
- a display/sound/video interface to present (e.g. display, listen to or visualize) the signer's document with the right format,
- an interface to get the signer information and the output status after signature verification,
- an interface to get the augmented Electronic signature with additional Validation data;
- an optional interface to write in a secure audit trail from an independent Trusted Third Party;
- a network interface to fetch information produced by Trusted Service Providers when not provided by the signer (e.g. CA repositories, CRLs repositories, OCSP responders, Time Stamping Authorities);
- an optional interface to get the definition of the Signature Policy (when the verification system is not only support dynamically programmable signature policies).



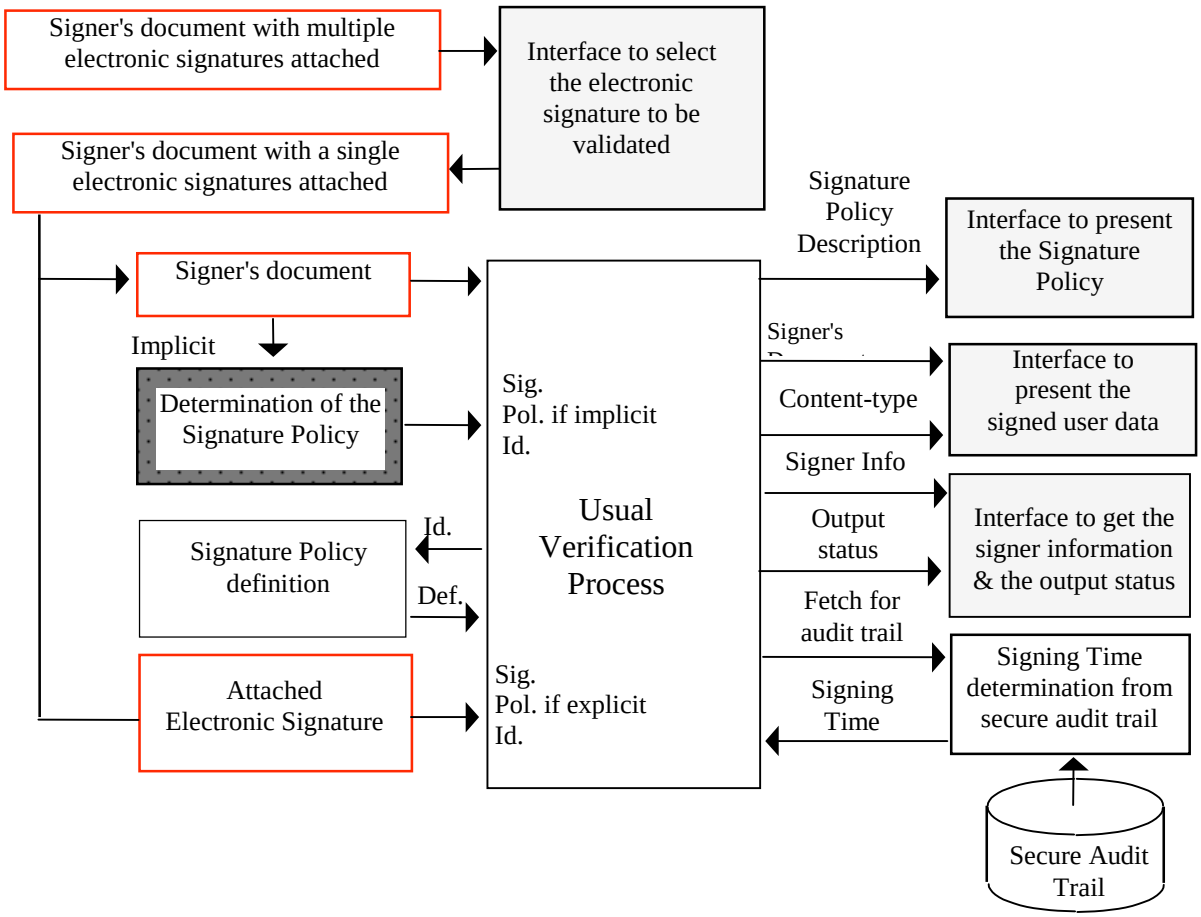
When the signature policy is implicitly defined, i.e. not explicitly defined within the electronic signature, the signature policy to be used during the initial verification process has to be determined by using a process which is outside the perimeter of the initial verification system.

When a Time-Mark, instead of a Time Stamp, then, one of the Trusted Service Providers must be in charge of keeping the electronic signature in a secure audit trail.

6.2. Usual Signature Verification system

A usual signature verification system is composed of :

- the secure signature verification process,
- an interface to enter the signer's document and to select the electronic signature to be validated (there may be more than one electronic signature attached with the user data),
- a display/sound/video interface to present (e.g. display, listen to or visualize) the signer's document with the right format,
- an interface to present the Signature Policy;
- an interface to get the signer information and the output status after the initial signature verification,
- an optional interface to enter the recording time of the electronic signature from the secure audit trail of an independent Trusted Third Party;
- an optional interface to get the definition of the Signature Policy (when the initial signature verification system is not only support dynamically programmable signature policies).



When the signature policy is implicitly defined, i.e. not explicitly defined within the electronic signature, the signature policy to be used during the initial signature verification process has to be determined y using a process which is outside the perimeter of the verification system.

When Time Marks, instead of a Time Stamps are used, then an interface to ask for an audit trail in order to determined using a process which is outside the perimeter of the initial signature verification system, the signing time.

6.2.1. Verification by a human

Humans will use various forms of implementations corresponding to the two generic diagrams presented before. The implementation will consist of several hardware components supporting software components.

Once an implementation has been installed, the whole system should not be able to be manipulated or disrupted without detection. This means that all the security comes from the installation phase, thenafter day to day use relies on the procedure of the installation phase and some means to make sure that this phase was correctly completed.

When using the signature verification system the user should be able to detect any security relevant system change to it since the system was installed.

Various user interfaces need to be present.

6.2.1.1.Interface to select the electronic signature to be verified

The signature verification system has to provide the user with a way to interact with it. When more than one signature are affixed to the signed data, this starts by indicating the number of signatures that possibly exist and offering which one has to be verified.

6.2.1.2.Interface to present the description of the Signature Policy which is applicable,

Using the interactive interface (e.g. keyboard, mouse, tactile screen) the verifier may then wish to see/listen to the text associated with the signature policy, i.e. the **field of application** of the signature policy which is a description of the expected application of this policy and the conditions that apply to the electronic signature, e.g that the signature complies to article 5.1 of the EU Directive.

6.2.1.3.Interface to present the signer's document

The user interface has to present the content of the signer's document in an appropriate way, so that a person verifying a signature SHALL also be able to identify the contents of the signer's document to an adequate extent. The signer's document may be text, voice and video, in many different formats. In order to select the right way to read, listen or visualise the signer's document, the presentation format of the data is always indicated within the electronic signature and that information is thus protected by the digital signature from the signer. This interface has thus to fulfil the requirement "**W**hat **I**s **P**resented **I**s **W**hat **I**s **S**igned" (**WIPIWIS**). If, for any reason, the content of the signer's document cannot be presented in exactly the right way, then the user interface SHALL clearly report this.

6.2.1.4.Interface to present the signer information and the output status,

The signer's identity, i.e. the name or the pseudonym of the purported signer SHALL be able to be displayed. That name is extracted from the information contained in the Distinguished Name of the signer's certificate. If the certificate has not be provided by the signer, the name of the CA should be displayed instead and if that name is acceptable, that certificate must then be fetched using the network interface. This name is only meaningful for the CSP which has issued the certificate, so the name of that CSP SHOULD be displayed with the name of the signer.

The following information SHALL be presentable at the wish of the verifier:

- the registered name or the pseudonym of the purported signer associated with the name of the CSP which has issued the Qualified Certificate (if not done before),
- the claimed date and time of the electronic signature, when present.

Using the interactive interface the user should be able to get additional information like:

- other content of the signer certificate,
- the date and time of the time stamp if present,
- the place of the signature (if present),
- the commitment type under that signature (if present),
- the claimed role or certified role under which the signature was generated.

Using the interactive interface the user SHALL be able to get the status of the verification process according to the signature policy. The output status SHALL be presented in a reliable, unambiguous and non-manipulatable manner.

The output status of the initial verification process can be:

- verification complete;
- verification failed;
- incomplete verification.

6.2.1.5. Interface to obtain the validation data

If the electronic signature appears to be conditionally valid (incomplete verification), the interface SHOULD propose to the user to capture the information to make it valid for the longer term.

6.2.1.6. User interface requirements

It is recommended to ensure user confidence in the electronic signature verification process by making the interface as easy to use as possible; by ensuring that the interface is accessible for all users, including people with special needs; and by reducing the probability of human error. In particular the dialogue system should:

- provide unambiguous user guidance based on relevant ergonomic standards/guidelines to cover how to use the signature verification system, and, if applicable, to install and configure the system.

- be self descriptive to the extent that each dialogue step is immediately understandable through feed back from the system or is explained to the verifier upon request.

- conform with usual verifier's expectations to the extent that it corresponds to the verifiers knowledge, education, experience and commonly accepted conventions.

- be adaptable to support the verifier's individual needs and preferences.

- be error tolerant if, despite evident errors in input, the intended result may be achieved with minimal corrective action.

- support informative error documents to lead the verifier forward.

- provide feedback to confirm that the action carried out by the verifier is correct (or incorrect).

- use standard conventions for the use of colours, e.g. red = error, green = go/proceed.

- be able, at any time, to cancel the current operation and return to the main menu; or, to exit the system completely.

- allow privacy for the individual, e.g. by making the information not accessible by others at the user interface.

- provide access to all people on equal terms if all people (including first time users, children, the elderly). Physically handicapped and visually impaired people might require specific verification systems.

6.2.2. Verification by machine

In contrast to the verification by human, the verification performed by a machine does not have a user interface. In this case signatures are automatically verified. The verification of electronic signatures is performed without direct user interaction. The result of the verification should be recorded and then be interpreted at any time later on.

For automated processing, Application Programming Interfaces (APIs) may be used. Although there are many ways to construct such interfaces, they may be split into two categories:

- ą APIs to extract the information contained in the electronic signature,
- ę APIs to verify the electronic signature and obtain the validation data.

The first set of APIs allows to extract the information contained in the electronic signature and obtain the format of the electronic signature. It is then necessary to make sure that this format is supported by the APIs able to verify the electronic signature. If the signature policy is implicit, then the context of use may define the signature policy. In such a case, a single signature policy will be used and the next set of APIs must support it. If the signature policy is explicit, it must be extracted from the electronic signature itself using the previous APIs. It is then also necessary that the next set of APIs supports this signature policy.

The second set of APIs allows to validate and/or verify the electronic signature and obtain the signer information, the output status and the validation data. While the first set of APIs only gives an hint about the information contained in the electronic signature, the second set provides a guarantee about this information.

Since there is no human being in front of the process, there is no need, in that case, for an interface to present the content of the signature policy, nor the content of the signer's document.

6.2.3. Verification by a Third Party

Verification may be sub-contracted to a third party. In such cases, the Third Party will perform the task and the requester must be sure that the task has really be performed by the Third Party as requested. A data authentication service with integrity check must be used so that it can be made sure that the result comes from the right source. Since the initial and usual verification processes are quite complex, this allows small clients (in the sense of a client/server model) to take benefit of the use of electronic signatures without the need to directly support all the complexity of these processes. For “light” implementations, it is even possible to directly install a public signature verification key from a Third Party, i.e. without supporting a CA hierarchy.

7. Examples of different user environments

Four main environments have been considered: the home environment, the office environment, the public environment and the mobile environment. The ways to meet an acceptable assurance level are not identical. Basically security is guaranteed by a combination of technical measures and of procedural or organizational measures. For each of these environments these two components exist but are not equally weighted.

The classification of the different environments is strongly related to the difference in the responsibility/liability for the various environments.

7.1.1. Home environment

In a private application environment, the user is provided with trust in his private equipment, because the equipment is either placed under its exclusive control or placed under the control of a small group of people who all trust each other. He may use various kinds of equipment, e.g.:

- a Desktop (PC),
- an interactive television (smart TV)
- a Network Computer,
- a Personal Digital Assistant (PDA),
- an Internet Phone.

The software able to verify electronic signatures will use and co-exist with other software (the operating system and the applications). It must be made absolutely sure that such other software is not malicious or cannot interfere with this software.

The software that verifies electronic signatures may be either pre-loaded by the user or downloaded at the time it is needed. In both cases, the user must rely on the source where from he obtained the software. However, the confidence is not obtained in the same way.

If pre-loaded, the confidence will comes both from the shopping place and the form of the package that contains the software. The package(s) should have a clear indication of the characteristics that are supported, in particular:

- which electronic signature formats are supported,
- which signature policies or which signature policy formats, are supported,
- which document formats, may be presented (WIPIWIS).

  Note: the two first characteristics may be combined, while the third one should be kept separate in order to be able to be upgraded to support new forms of documents.

The packages should also have a clear marking that they fulfil the requirements laid down in the present document. This could be achieved by using a logo.

Then the user needs to install the software. In order to increase the level of security, the equipment could, in addition, contain a public key used to verify that the software being loaded is correctly signed.

If downloaded at the time of verification, the confidence comes from the fact that the software is signed and that the latest version is being downloaded. The security of the downloading process relies on a public key that is provided with the equipment or that is installed once by the user.

Since the user directly participates in the installation, he is directly responsible to verify that the correct procedures have been followed.

Once the installation has been performed, the user must make sure that no one can modify the installed software, without this being detected. This may be achieved by using only physical security (e.g. a door lock) or a combination of physical security and software (e.g. boot-protection, anti-virus, hard disk encipherment).

7.1.2. Office environment

In an office environment, the organisation the user belongs to has the responsibility to provide the adequate tools for day to day working. The user may use various kinds of equipment, e.g.:

- a Desktop (PC),
- a Laptop,
- a Personal Digital Assistant (PDA),
- a Mobile Phone.

The software able to support the functionality may be either pre-loaded by the people in charge of the user's equipment or downloaded at the time it is needed.

In the first case, the organization must rely on the source where from it obtained the software. The confidence will come both from the shopping place and the packages that contains the software. The package(s) should have a clear indication of the characteristics that are supported, in particular:

- which electronic signature formats, are supported,
- which signature policies or which signature policy formats, are supported,
- which document formats may be presented (WIPIWIS).

The packages should also have a clear marking that they fulfil the requirements laid down in the present document. This could be achieved by using a logo.

Then the people in charge of the user's equipment need to install the software. This can be down locally on each equipment by downloading the software from a trusted server from the organization or be done remotely.

In the second case, the user must rely on the source of code that is provided externally. That code must be signed and it must be made sure that the latest version is being downloaded. The security of the downloading process relies on a public key that is provided with the equipment or that is installed once by the people in charge of the user's equipment.

Since the user does not directly participates in the installation, he is not directly responsible to verify that the correct procedures have been followed. However, it might have the possibility to modify the software afterwards. This capability depends from the operating system being used, in particular whether it makes a difference between administrators and users.

Once the installation has been performed, the organization must make sure that no one can modify the installed software, without this being detected. This may be achieved by using a combination of physical security and software (e.g. boot-protection, anti-virus, hard disk encipherment).

7.1.3. Public environment

In a public environment, the organisation to which the verification system belongs to has the responsibility to provide a trustworthy system. The user may use various kinds of equipment, e.g.:

- a retail Point-of-Sale (POS),
- an Automated Teller Machine (ATM),
- a public service point.

The installation phase must be carried out under the responsibility of the organisation owning the system, which means that the name and address of that organization must be clearly identified on the system itself. Means to reach that organization by phone, surface mail, E-mail or web should be indicated. The organization must then make sure that no one can modify the installation without placing the system out of service.

The user will get confidence in such a system not only because it will look like a "real" system which bears a clear marking (e.g. logo) of what it is intended for, but also because it is placed in an environment where it would be difficult, without being noticed, to install a fake system.

In order to educate users with the view of “real” systems, users should be advertised personally or/and through the press of such an appearance.

7.1.4. Mobile environment.

In a mobile environment, some equipment that may be used as a stand alone device and are already considered in an office or home environment may be used, e.g. a LapTop connected to a telephone line. Although the delimitation between stand alone systems and systems that only work connected is hard to denote (e.g. a Personal Digital Assistant (PDA) connected or not to a phone line), some devices are meant to be used in a connected environment, e.g. a mobile phone. In such a case, the user is provided with trust in his private equipment, first because the equipment is provided by a manufacturer which SHALL provide some assurance about the properties of the device. Secondly, because the device then is placed under the exclusive control of the user, who is going to personalize the equipment with user specific data, e.g. stored in a SIM card.

The verification software able to support the functionality may either be put on the device by the manufacturer, be installed by the user or be downloaded at the time it is needed (e.g. using MExE). MExE has an architecture for verifying downloaded content which is itself based on digital signatures. The user therefore relies on the source of the software for its content, but can be given assurance as to the integrity and authenticity of the content by software that the terminal manufacturer has put on the device.

The downloaded software may be provided by the phone company and the security of the loading may then come directly from the protocol being used between the mobile equipment and the network. Alternatively, this software may be provided by a content provider and the security of the loading may then come from the security of the proxy server (e.g. when WAP is used).

In order to authenticate the software some root keys will have to be used. They may be manually installed by the user. This may be done by fetching the information from some place and then verifying that the hash of what has been downloaded matches a hash value provided by out-of-bands means. They may also be put on the device by the manufacturer (WAP handsets will have pre-installed roots by the end of the year) or on the SIM or WIM. User download is what currently happens but its just for the short term. The WAP WPKI specification gives two ways of downloading roots, either signed by an existing root or using hash verification, but with the device, and not the user, comparing the expected and actual root hashes.

The software that has been installed or downloaded shall then have the properties to authenticate the source of the signature policies.

8. Requirements for signature verification systems

8.1. Scope

All components of the signature verification system that interact with the Secure Signature Verification Process (see Chapter 6) should be realized in a Secure Area.

Note: A Secure area is an area within a component in which the storage and processing of data and the processes within this area are protected against successful manipulation by means of special measures.

As regards the degree of protection that can technically be achieved and the risk management applied by the verifier, the following three different levels of implementation should be considered:

- In a **Software Module** the security measures are implemented in software. The security that can be achieved in this way depends on the security of the operating environment. Especially for a PC with a standard operating system, adequate protection of data and processes by means of security measures implemented in software is a controversial topic among experts.

- In a **Tamper-evident module** security measures are implemented in such a way that, although manipulation cannot be prevented, the user can detect it. This means that a user can be prevented from unwittingly using a component of which the secure area has been manipulated. For a PC with a standard operating system, a tamper-evident module is only technologically possible at present using additional hardware.

- In a **Tamper-resistant module** security measures have been implemented in such a way that manipulation are not possible without unreasonable effort. The effort required for manipulation should be considered against the benefit derived from such manipulation. Such modules are presently only possible by using special hardware. A **Security module** is a component that as a whole constitutes a secure area created by means of a tamper-resistant module.

A mix of these different modules may be used to build a signature verification system. It should be noted that the overall security of the system is equal to the lowest security level of any of these modules.

8.2. Hardware and software requirements for tamper-evident and tamper-resistant modules

1. At the time of installation the integrity and authenticity of hardware and software should be ensured for all components.

2. Security-relevant data and processes in secure areas should be protected against unauthorised modification by means of the following measures:
   - Implementing design-inherent security characteristics in software and hardware being used in secure areas.
   - Loading security-relevant software into the secure area at the time of manufacturing the secure area or, during operation, protecting the security-relevant software by cryptographic means.
   - Protecting the loading of security-relevant data, particularly of cryptographic keys that are stored permanently in a tamper-resistant module, by cryptographic means.

3. Modifications of secure area hardware components should be recognisable.

Notes to requirements 1, 2, and 3:

a. The security-relevant data and processes to be protected in a secure area include, in particular, root public keys and program code.

b. If a secure area is created by means of a tamper-evident module, the design of the software and hardware SHALL ensure that attacks can be recognised. This SHALL be achieved by ensuring that:

- data and processes in the secure area can only be manipulated once the hardware protective cover has been opened,
- any opening of the hardware protective cover can be recognised after the cover has been closed.

c. If a secure area is created by means of a tamper-resistant module, the design of the software and hardware SHALL ensure that successful attacks are not possible without unreasonable effort. The effort required for a successful attack SHALL be weighed up against the benefit derived from such an attack. The protection SHALL be achieved by ensuring that:

- data and processes in the secure area can only be manipulated once the hardware protective cover has been opened and
- both mechanical and electronic storage protection are used to protect data and processes.

A tamper-resistant module SHALL protect data and processes in case of destruction of (parts of) the module by irretrievably destroying the data and processes.

d. Hardware modifications include the addition of further components.

e. Special hardware may include data input and display components.

4. If the signature verification system is under the control of the verifier, then:

- the supplier should provide protection profiles for the different types of risk management (scalability of security),
- the security target based on the protection profile should specify which security requirements are met and which are not met.
- the supplier of hardware should provide evidence to the verifier that the hardware is appropriate for electronic signature verification systems and meets the security requirements,

the supplier of software should provide evidence to the verifier that the signature verification software meets the security requirements,

5. If the signature verification system is under the control of a Service Provider and offered to the public, then
the supplier SHALL provide evidence to the Service Provider that the signature verification system meets security requirements as stated by the Service Provider,
the Service Provider should provide evidence to the verifier that the security target specifies which security requirements are met by the signature verification system.

8.3. Assumptions concerning installation and verification of signature verification systems

The components of the signature verification system may be implemented using a combination of trusted devices and other hardware and software. A trusted device is tamper-evident or tamper-resistant (refer to section 11.2).

The other hardware and software components may present various levels of security. In any case the security should first of all rely on a form of physical security. This may be obtained by placing the equipment in a presumably safe area, e.g. a home or a office. Alternatively, access security may be used to ensure that, after installation, what has been installed has not been modified. As an example, any access to a PC may need supplying a password. If the PC is provided with a lock, then changing the initial password becomes unlikely. If the PC is not provided with a lock, then any unauthorized access to the PC can be detected, because the password can be changed, but is unlikely to be set back to its initial value, due to the provision that the password can only be set, but cannot be read.

Continuous checking that the software is as it should be may be provided in two ways:

- using a virus protection program and only loading other programs from trusted sources,
- using the initial media used for installation to verify that the installed software remained unchanged.

Software providers of signature verification systems should provide the tools to perform such checks at any time after installation.

Once a verification system has been set up, the user must be able to detect any manipulation before performing the signature-verification process. This leads to the requirement in section 11.2 that security-relevant changes in components must be apparent for the user. Users must be able to verify the authenticity of these components at the beginning of use, in order to prevent "duping" with false data via manipulated technical components.

8.4. Requirements for signature verification systems and processes

The signature verification system should meet stated security objectives to guarantee the assurance for the whole system. The system consists on one side of the secure verification process (with its inputs and outputs) and on the other side of several interfaces.

The interfaces (whether human interfaces or programming interfaces) of an initial or usual signature verification system are used to present various information, including the output status to the signer.

The additional interfaces (whether human interfaces or programming interfaces) for a verification system are only used to provide for augmented electronic signatures.

In the case of machine verification, the selection of the electronic signature to be verified is done by an application, while the presentation of the signer's document and of the Signature Policy are only done in the case of the presence of an individual.

The specific requirements to be met by a component are the same, but different realisations of the components provide different levels of confidence in the implementation, subject to the environment where these components are applied. Generally the entire system should be secure, which means that any information that is obtained from the whole system should be accurate.

8.4.1. Verification process

The verification process SHALL verify the electronic signature according to the rules of the signature policy. The specification of the rules to be followed when verifying a signature is a subset of the signature policy, i.e. the signature validation policy. The secure signature verification process SHALL fulfil the specified rules in a demonstrable way. These requirements SHALL be suitable to meet the objectives defined in the signature validation policy. The conditions defined in section 5.5 SHALL apply.

8.4.1.1. Processes with built-in signature policies

Each signature verification process must be evaluated against each security policy that is claimed to be supported by the system. Each signature policy indicates which cryptographic algorithms are supported.

8.4.1.2. Processes using externally described signature policies

Each signature verification process SHALL be evaluated once against the security policy descriptive language. Since the policy is described in a machine processable language, the description of that policy in that language should first be interpreted (e.g. compiled). In addition manual checking SHALL be provided to ensure that the parameterisation that is used corresponds to a valid description of a policy.

In order to perform checking of the verification process, a set of test signature policies may be used against a set of electronic signatures to be verified.

8.4.2. Interface to obtain the definition of the Signature Policy

If the verification system supports programmable Signature Policies, then during the verification process the authenticity and the integrity of the Signature Policy SHALL be ensured.

If the verification system supports fixed Signature Policies, with some elements externally defined (e.g. root keys) then during the verification process the authenticity and the integrity of those elements of the Signature Policy SHALL be ensured.

8.4.3. Interface to select the electronic signature to be verified

The interface should allow the verifier to select the signer's document to be verified or both the signed document and the electronic signature to be verified.

8.4.4. Interface to present the applicable Signature Policy

The interface should present to the verifier in a reliable, unambiguous and non-manipulatable manner the identifier of the signature policy and content of the field of application from the signature policy, which is a description of the expected application of this policy and the conditions that apply to the electronic signature.

8.4.5. Interface to present the signer's document

The interface SHALL present to the verifier in a reliable, unambiguous and non-manipulatable manner an unambiguous signer's document, i.e. the content of the signer's document to an adequate extent. The signer's document may be text, voice and video, which may be viewed, printed or listened to.

8.4.6. Interface to present the signer information and the output status

The interface SHALL present to the verifier in a reliable, unambiguous and non-manipulatable manner the name of the signer. The name SHALL be extracted from the information contained in the Distinguished Name of the signer's certificate, together with the name of the CA. Other information like signing time, signer location, commitment type and roles, when present SHALL also be presented, when present. The output status of the process SHALL be presented.

When initial verification is performed, one of the following three statuses SHALL be presented:

- verification complete,
- verification failed,
- incomplete verification.

When usual verification is being performed, one of the following two statuses SHALL be presented:

- verification complete,
- verification failed.

8.4.7. Interface to ask for an augmented electronic signature

This interface is specific to the initial verification process. When there may be a need for a subsequent usual verification, the interface SHALL allow the verifier to request capturing of information that would make the electronic signature valid for the longer term. In that case, the initial verification process SHALL provide the corresponding output.

9. Conformity assessment

Formal conformity assessment of signature verification devices is not possible, since this document is only a set of guidelines. However, this document may be used as the basis for confirming that a signature verification device meets the requirements identified in this document.

Instead of a formal conformity assessment, a conformity declaration that an operational device is following these guidelines may be used. Such declaration will be different whether the signature verification device is directly under the verifier's control or under an organization's control (e.g. a device in a public environment).

In the former case, a supplier’s declaration of conformity will be sufficient, while in the later case, two declarations will be needed:

1. one provided by the manufacturer of signature verification device, and
2. one provided by the organization responsible for the installation and management of the device.

The supplier’s declaration of conformity is provided by the manufacturer of the signature verification device itself. An independent body may provide a certificate based upon a voluntary product certification scheme for signature verification devices. In either case, the declaration should explain how the requirements are met.

When a certificate is provided by an independent body, the certificate may be based upon an appraisal of the signature verification devices by an evaluation team deployed by the independent body. The evaluation team performs appraisal of the documentation and operation of the signature verification devices against the requirements of this document and reports its observations. The independent bodies responsible for performing conformity evaluation should make public statements of the capabilities of signature verification devices whilst permitting the manufacturers to keep details of their internal processes and information security measures confidential. Note that due to the lack of an agreed interpretation of the requirements, independent bodies might arrive at different conclusions when evaluating the same signature verification device.

Conformity declaration of signature verification device by the manufacturer is voluntary. However, public confidence in the trustworthiness of signature verification devices would be provided to users when the signature verification devices have successfully passed the evaluation process.

In the same way, conformity declaration of signature verification device by organizations responsible for the installation and management of the device is voluntary. However, public confidence in the trustworthiness of signature verification devices placed in public areas would be provided to users when the signature verification devices that have been installed have successfully passed the evaluation process.

To this respect organizations in charge of signature verification devices placed in public areas might find useful to fix a logo on the signature verification devices which will indicate that the device meets the requirements identified in this document.

10. Legal Aspects

10.1. Legal invalidity of a “technically correct” signature

According to the Directive, advanced electronic signatures which are based on a qualified certificate and are created by a secure-signature-creation device are deemed to satisfy the legal requirements of a signature in relation to electronic data, in the same manner as a hand-written signature satisfies such requirements in relation to paper-based data. Advanced electronic signatures should be admissible in legal proceedings and in any other function where currently hand-written signatures are mandated. Such signatures would be "technically valid", i.e. the digital signature is correct, the certification chain is correct, none of the certificates in that chain is revoked, etc.... However there are cases where an electronic signature, which is attributable to a signer can be overcome by means of counter-proof.

As with hand-written signatures, the usual verification of a signature according to a specific signature policy could be associated as a rebuttable presumption that the signature is valid. Hence, in case of a dispute, counterproof may be provided by any party with regard to the legal validity of a “technically correct” signature. The invalidity of a signature may be decided by a judge who should determine the conditions of signing or the type of the transaction. Those conditions are not necessarily related to the compliance of the signature with pre-defined technical standards while conditions may depend upon such debatable factors as the application field, the type of the transaction, the conditions of usage, trade practices etc.

Consequently, a signature can be valid under suspensive conditions, which may be attributed to the signer, to the type of commitment made under the signature policy or to the number and sequence of signatures required by Law to establish the validity of a certain transaction.

- Suspensive conditions related to the signer are applicable when the signer acts under constraints, (e.g. under threat), he has limited mental capacity (e.g. lacking the capacity to consent to a contract), or when he can prove that the signed data have been incorrectly presented to him, because for instance his browser could not read the entire set of signed data which contained hidden text.

  National laws contain provisions, by virtue of which a person who has been forced to make a declaration of will under threat used unlawfully or in manner contrary to morality by the other party or by a third party may claim the annulment of such a transaction.

- Suspensive conditions related to the type of commitment made under the signature policy e.g. a certain signature policy used only in a certain business environment (e.g. car rental) has been used for a signature of a contract situated outside its scope (e.g. for a real estate contract).

- Suspensive conditions related to the lack of a signature in case that more that one parallel signatures are required e.g. in corporate law, the company articles of incorporation may state that a payment exceeding a certain amount can only be validly performed if signed by both the accounting director and by the head of the procurement department.

- Suspensive conditions related to the sequence of embedded signatures that may be required in a specific legal context to make a transaction valid (e.g. real estate contract); in such a case, a notary public may have signed electronically and accordingly ‘‘closed’’ the notarial deed without having previously including the signatures of the seller and the buyer. This implies nullity of the contract although signed by three ‘‘technically correct’’ signatures affixed to the document in the wrong sequence.

Special attention is required for the conditions under which certain types of contracts might be concluded. As the law requires a higher level of assurances prior to concluding an insurance contract or a real estate contract that include affixing a hand-written signature, such transactions have been excluded from the scope of the Directive 99/93. To affirmatively respond to the conditions necessary for such transactions to take place electronically, further investigation is essential.

10.2. Risks related to certificate revocation

Reporting change of status on a digital signature is a risk that is shared between the subscriber of a digital certificate and a relying party making use of such certificate. As soon as a subscriber realises a change in the status of the digital signature (e.g. theft, loss or compromise of the private key) he has a duty to report it immediately to the CSP. The CSP has a certain time frame at its disposal to update the status of the certificate in a publicly available repository, using either revocation list (CRLs) or an OCSP server. Typically, CRLs are updated periodically while OCSP systems are real-time. The conditions of usage of a Repository are appropriately stated in the Certification Practice Statement of the CA.

A positive verification may only be obtained after the expiration of a reasonable cautionary period, which may be specified in the signature policy. If the certificate is revoked after the expiration of that pre-defined cautionary period the signer may held liable for any losses sustained, unless a suspensive condition applies.

However, if the cautionary period is not defined in the signature policy, then the verifier should refer to the CPS from the CA corresponding to the CP for the certificate of the signer. In order to perform verification, he should add the maximum time for the CA to make available revocation status for certificates to the maximum time for a subscriber to report revocations after a key compromise has occurred.

When such information is not present, then verification may not be reliably effected. Accordingly, the verification process should end up with "incomplete verification", leaving the risk to the verifier to accept or reject an electronic signature. The introduction of technologies providing real-time certificate revocation status for enhancing the use of PKI in time-critical applications (e.g. auctions, stock market etc.) solves only partially this problem, since it does not reduce the time for subscribers to discover that their private key has been compromised.

Signers also run a risk of denial of service when a person who is not entitled to ask for a certificate to be revoked, succeeds to obtain a certificate suspension or a definitive revocation. To avert such risk CAs should put in place robust security infrastructures and access control mechanisms.

In situations where a person other than the certificate owner requests a certificate revocation, there must be a reliable means for the CA of identifying the requestor and determining whether the requestor has authority to request revocation.

Signers also run a risk of loss when the CA fails to make available revocation status for a certificate in due time.

Various legislative solutions may be applied for managing legal liability uncertainty: the technology - specific approach, the two tier approach and the minimalist or technology neutral approach (B.P Aalberts, S. van der Hof -Digital Signature blindness, analysis of legislative approaches toward electronic authentication, November 1999, available at *http://www.kub.nl/~frw/people/hof/ds-fr.htm*).

The Directive adopts the two tier approach : Tier 1 provides legal recognition (e.g. for form purposes) of a wide range of electronic signatures and Tier 2 provides special legal consequences (often relevant to liability allocation) for PKI digital signatures or “secure electronic signatures’’.

Broadly, there are three methods to manage legal uncertainty concerning certificate revocation in a PKI :

- Private law mechanisms, such as use of non-contractual disclaimers (e.g. a statement on a CRL website or in the certificate that users rely on the contract at their own risk), contractual provisions allocating risk between parties to the contract and insurance against such risk.Limiting the reliance limits on a certificate may proprtionally reduce the amount of Trust that a subscriber or a relying party may put on it.
- Wait for test cases to clarify the application of existing legal rules to legal liability issues that are currently uncertain.
- Legislate or regulate new legal rules to reduce or eliminate areas of uncertainty in the existing law.

10.3. Dispute settlements

Legal disputes surrounding electronic signatures may arise when one party attempts to prove or disprove the existence of a contract. The primary issues to be tackled by the verifier are related with the validity of the private key at the time of the signature.

In case of a compromise of the signer's key, the date of revocation of the signer's key can be compared with the date of the time stamp or of a time mark.

Firstly, if the date of the time stamp or time mark is earlier than the date of revocation, then it proves that the signature was applied before the revocation of the private key and hence the signature is valid. Otherwise the signature is invalid.

Secondly, the cautionary period must be considered to allow to time to report and publish certificate revocation status information, this means that, in addition, the difference between the date of the time stamp or time mark and the date of revocation must be greater than the cautionary period.

If there is no such a time stamp or time mark or if their dates are later than the end of the period of validity of the certificate, then the electronic signature is invalid.

In case there was no compromise of the signer's key reported during the validity period of the certificate, it is necessary to prove that the signature was performed before the end of the validity period of the certificate (because the CA does nor make any reporting of key compromises of the end of the validity period).

Considering the substantial amount of complexity to handle such cases further attention can be given to mechanisms supporting on line Dispute Resolution.

The legislator might decide to use the general rule: "a contract is formed when both parties are aware of each other's consent", there should be the definition of the place where the proponent has cognisance of the acceptance through affixing its signature.

This place may be important when the choice of forum is dependent upon the signer's location. However, this place may alternatively be defined in the security policy and take into account some other parameters, like the jurisdiction competent for the home of the signer.

The recently adopted Electronic Commerce Directive introduces the Brussels Convention criterion for the settlement of a dispute, which is the place of residence of the consumer.

10.4. Consumer protection

In addition to the questions raised above, if the signed document is a "B to C" transaction verification involves several consumer protection aspects

The consumer protection measures adopted by the European Commission should be applied in the context of signature verification. In this respect, the recently adopted Electronic Commerce Directive, the OECD recommendations on consumer protection as well as with the Distance Contracts Directive (EC/97/7) contain provisions ensuring that:

- Reliable information is provided to the consumer both before and after the conclusion of the contract. This provision raises in turn the issue of availability and accessibility to the content of signature policies, for both signers and verifiers. In addition, CSPs from CAs must also be available to signers, verifiers and signature policy issuers

- A right of withdrawal allowing him to renounce within seven (7) working days to the contract without penalty and without justification. For goods this periods starts from the day of their receipt by the consumer, for services its starts form the day the contract was concluded or from the day confirmation was received. The Directive envisages a further respite of three months where confirmation has not taken place.

- This right of withdrawal may not exercised in certain cases, such as when for instance performance has begun, with the consumer's agreement, before the end of the seven working day period. This exception is particularly aimed at on line services (audio, video recordings, computer software etc) which are downloaded, the very nature of which does not allow restitution.

- Moreover, national consumer laws, as for instance the German "Law on revocation of contracts concluded door-to-door" give consumers a wide-ranging right to revoke such contracts within a certain

time limit. Similarly French regulations governing the use of electronic signatures for remote transactions (B to C) allow the buyer to deny the purchase within eight days.

Consequently, in order to comply with EU and national consumer legislation, the signature policies should satisfy the legislative requirements for balanced liability allocation and user security. To this end, it is useful to set up specific risk attribution rules taking into account the different bargaining position of parties in each business context, more than general legislative rules which apply to a wide variety of data documents. Those rules should also include the consumer rights for prior information, withdrawal and repudiation.. Finally, liability caps and reliance limits for certificates should be fixed, so as to assist consumers in evaluating levels of risk and making rational reliance decisions.

10.5. Data protection

From a data protection perspective, signature verification implies access by the verifier to some of the registration information provided to the CA by the subscriber. This information SHALL be first available to the subscriber upon his request. In addition, the delimitation of the other persons (judges, notaries, expert witnesses) allowed to legitimately obtain this information remains a delicate issue.

By virtue of the EU data protection directives (95/46/EC and 97/66/EC) and national laws, verifiers should be allowed to use only the personal data of the signer, which are needed on purposes of the task accomplished. Those data must be obtained directly from the signer or by any third natural or legal person such as the CA with the signer's consent. They must not be processed for purposes incompatible for which they have been initially collected. The purposes in question must also be explicit in the eyes of the data subject.

Nevertheless, if for whichever reason (buy out, bankruptcy, liquidation etc) the CA ceases to exist etc) the personal data collected at the time of registration or re-issuance of a certificate have to be transferred to a third party that supports trusted archival. According to the data protection legislation, in order to be legal, the specific authority to which the date will be transferred in case of cessation of activities of the CA, has to be specified in advance and be made with the person's consent. A general contractual clause allowing the transfer to any third body not specified form the outset would not be acceptable. This means that the person's consent must be obtained at the time of registration, otherwise registration should be refused. Consequently, it is necessary to provide in the relying party agreement for a pre-designated "default" trusted data centre, to which the personal data collected at the time of registration or re-issuance of a certificate will be transferred in such a case. National authorities might have to care for the existence of such a centre.

10.6. Verification of data incorporated by reference

In order to reliably establish the contents of the signed data, the verifier or any third arbitrator should be able to retrieve without any ambiguity the signature policy which has been used by the signer in the specific context and time of signing, in accordance with Annex IV of the Directive.

To this end, trusted repositories of registered model signature policies of standardised content should be used. Governments, banks, insurance companies, professional and trade associations should be encouraged to draft signature policies and standard agreements to be used by business partners for electronic transactions.

Such repositories have already been developed in the framework of open EDI and electronic commerce as for instance the ETERMS Repository or the GUIDEC developed by the International Chamber of Commerce (ICC). The purpose of those applications is to make publicly available a data base of legal and commercial terms which can be referred to by using uniquely coded identifiers and be incorporated in an electronic document by mere reference (Mitrakas – Open EDI and Law in Europe, 1997).

During the verification process, the verifier should be able to access the repository, establish the contents of signed data (language, format, warnings, disclaimers towards the parties included in the signature policy which is incorporated via a hyperlink into the signed contract etc), detect any changes (format, content, language etc) and also retrieve without any ambiguity the version of the signature policy in force at the time of the user's assent.

11. Multiple Signatures

Some electronic documents may only be valid if they bear more than one electronic signature. This is the case generally when a contract is signed between two parties. The ordering of the signatures may or may not be important, i.e. one may or may not need to be applied before the other.

Several forms of multiple and counter signatures may need to be supported. They fall into the following categories:

* independent or parallel signatures;
* embedded or wrapping signatures;
* overall signatures.

Independent signatures are parallel signatures where the ordering of the signatures is not important. The capability to have more than one independent signature over the same data should be provided. An electronic document with more than one independent signatures one can just imagine as a collection of a signed signer's documents with identical primary electronic documents and therefore the same hash value. Whether or not the other signature attributes must coincide more or less depends on the signature policy. Independent signatures (i.e. parallel signatures) may be selected by using the interface able to select the electronic signature to be verified.

Embedded signatures are applied one after the other and are used where the order the signatures are applied is important. The first signature is called embedded and the second is the wrapping signature. The electronic document for the latter is the digital signature of the embedded signature only. The wrapping signature is therefore an unsigned attribute for the embedded signature but must be verifiable by its own.

The embedded signature from the lowest level must be selectable, then wrapping signatures when they are present should also be selectable and verifiable independently.

Overall signatures differ from embedded signatures because the input for the signature is not only a previous signature but also the document itself. Overall signatures are used when the cryptography becomes weak and for archiving purposes.

These different situations may be illustrated as follows, using the following notation:

- the signer's document is called M,
- the signer's information from A that includes the attributes signed by A is called A,
- the signature S = sig (M,A) is computed on both a hash of M and A.
- the overall signature OS = sig (M,S,A) is computed by A on both a hash of M and a signature S on that document.

Parallel signatures

S1, S2 and S3 are parallel signatures of the document M : S1 = sig (M,A1) S2 = sig (M,A2) S3 = sig (M,A3)

Counter signatures

S2 and S3 are a counter signatures from A2 and A3 respectively of the document M previously signed by A1: S1 = sig (M,A1) while S2 = sig (S1,A2) and S3 = sig (S1,A3)

S4 is a counter signature from A4 of the document M previously signed by A1 and counter-signed by A2: S1 = sig (M,A1) with S2 = sig (S1,A2) and S4 = sig (S2,A4)

Overall signatures

S2 is an overall signature from A2 of the document signed by A1 where the signature is made both on the original document M and the signature from A1 over that document. The signature algorithm used for the overall signature from A2 (more precisely the hash function) is normally stronger than the one from the previous signer.

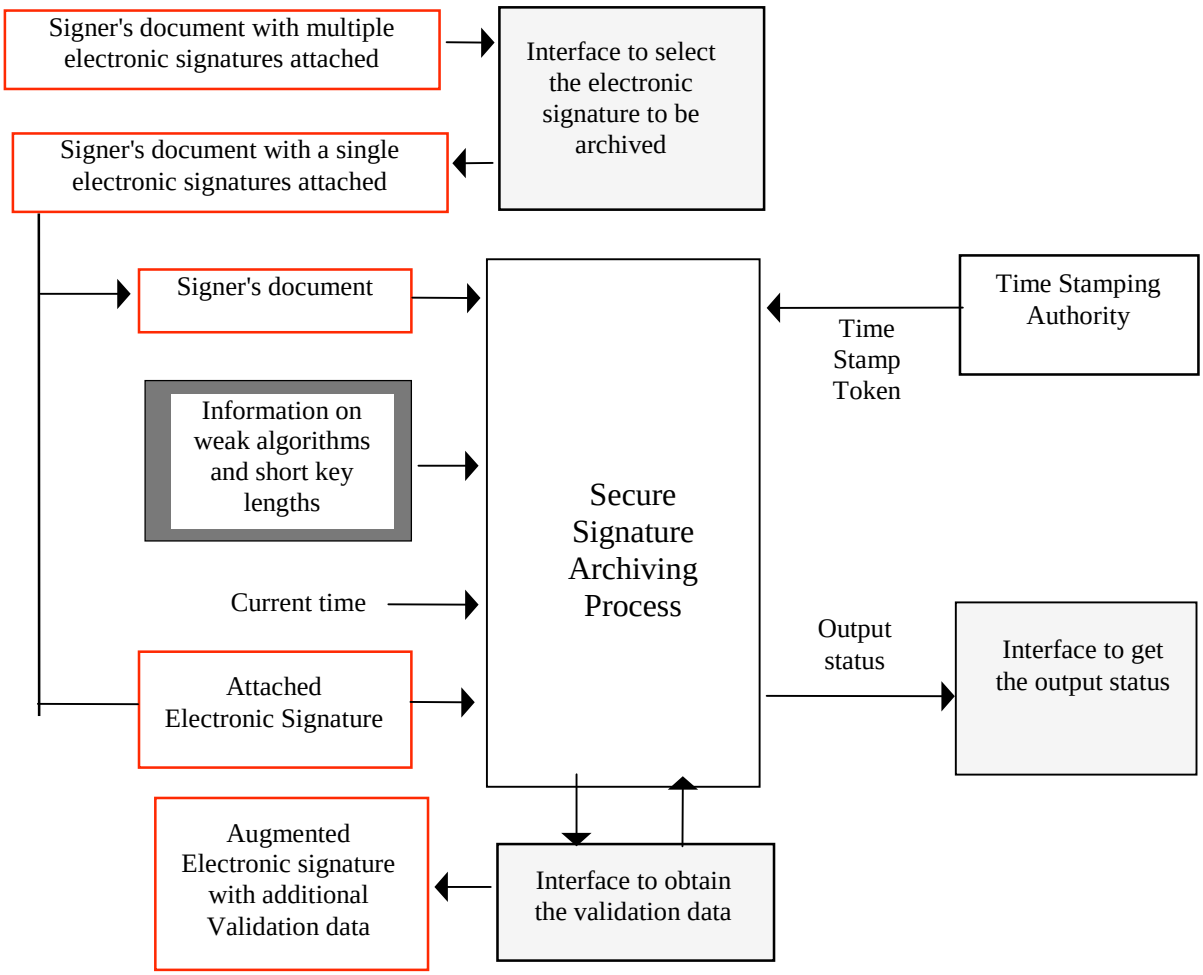
S1 = sig (M,A1) with OS2 = sig (M,S1,A2)

12. Archive system

An Archived Electronic Signature is a form of signature that consists of both the Signer's document and an Electronic Signature with additional validation data, i.e. a time stamp. This form is necessary if the hash function and the cryptographic algorithms that were used at the time of the signature are likely to be no longer secure at the time of a later verification. In that case the hash function used by the Time Stamping Authority will have to be secure.

An archive system is composed of :

- an interface to enter the signer's document and select the electronic signature to be archived (there may be more than one electronic signature attached with the user data),
- an interface to obtain a trusted copy of weak algorithms and key lengths as well as good algorithms and key lengths;
- a network interface to fetch information produced by CSPs, i.e. Time Stamp Token form a Time Stamping Authority, when it becomes necessary to extend the life-time of the cryptography.
- an interface to know whether the electronic signature needs to be updated or not.
- an interface to obtain the updated validation data.



The process may need to be performed and iterated before the cryptographic algorithms used for generating the previous time stamp are no longer secure. An Archived Electronic Signature may thus bear one or more time stamps.

13. Annex A: Annex IV from the Directive

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

(a) the data used for verifying the signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of that verification is correctly displayed;

(c) the verifier can, as necessary, reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

(e) the result of verification and the signatory's identity are correctly displayed;

(f) the use of a pseudonym is clearly indicated; and

(g) any security-relevant changes can be detected.

14. Annex B. Continental versus Common Law

Informative

A.1. Continental versus Common Law

Among other functions, a hand-written signature expresses a declaration of will of the signer to be legally bound under specific terms and conditions at a certain time and place. When signed, the document becomes attributable to the signer. The signed document is deemed to reflect the facts correctly, unless evidence to the forgery, invalidity or nullity of the document is produced. Signed documents may be also be used as evidence of the transaction.

A signature is not part of the substance of a transaction, but rather of its representation or form. Requirements of form are very different in various legal systems. Contract law enjoys the principle of freedom of form and party autonomy. This means that for validity purposes, the contract can be concluded orally or in any way including electronic form. However, in order to be enforced the contract has to be proved. The rule of evidence and the requirements of form are different in civil law countries and in common law countries.

A.1.1. Civil law

In civil law countries (e.g. Germany, France, Greece, Italy, Portugal, Spain), the production of evidence is related to rules which regulate the conclusion of transactions and the storage of documents. Several types of evidence apply:

- ‘‘Rigid or procedural evidence’’ expects evidence to be produced by the evaluation by the judge of specific means of proof enumerated in national codes of Civil Procedure;

- ‘‘Free evidence’’ is a system where evidence may be produced through any appropriate means under a flexible procedure;

- ‘‘Partly free evidence’’ is an intermediary type of evidence. This allows the evaluation of means of proof that should not normally be admissible by the codes, where it does not completely relieve the court of certain rules on rigid evidence.

According to civil law systems, a signed original document is required so as to establish evidence acceptable by courts in case of litigation. Documentary evidence produced through a written document to which a hand-written signature is affixed has the benefit of constituting in most cases a reliable means to prove a disputed fact. Many current national laws require that some documents (VAT documentation, tax returns etc) should be drawn, transmitted and stored on signed original papers.

An original of a document (official act, private contract, deed poll ‘‘inter vivos’’ or ‘‘mortis causa’’ such as a testament; etc) is the writing signed by its originator. All its reproductions are copies. Each legal system assigns a different value to a copy, depending on its character as simple copy or faithful copy.

However, this requirement for written evidence is not mandatory in all cases. Parties are entitled to agree in advance that the contracts they will agree upon will be proved by other means, such as parole evidence. Their agreements will contain an appropriate provision on the record of the transaction which would be used as evidence. This provision can take the form of general conditions, enforceable in individual transactions.

In civil law countries the introduction of a system of electronic document signed with a digital signature presented serious problems, which suggested the need for new law.
Most EU countries have already a law (Austria, Germany, Italy, France, Spain) or a draft law (Belgium, Denmark, Finland, Greece, Netherlands..) or plan to revise their legislation in compliance with the EU Directive (e.g. Germany).

A.1.2 Common Law

In Common Law countries (e.g. UK and Ireland) the meaning of requirements of form is different than in civil law countries. Rather than on the security of the signing process, the emphasis is on the signer's intention to be bound (Kuner & Miedbrodt 1999). As an additional requirement, the signature must be recorded on a tangible medium. If these factors are satisfied, a signature will be considered legally valid.

Any kind of mark is acceptable provided it is affixed by the person or by some other person authorised by the person intended to be bound. Unless there is some specific legislative requirement the mark can be affixed by some mechanical means and can be located anywhere in the document (with some exceptions introduced by legislative requirements of form as in a will, specifying where the signature has to be placed).

The rules of evidence raise a number of problems in common law countries, because of the existence of two rules which emphasize the need for reliable evidence, e.g., the "Best evidence" rule and the rule against "Hearsay". In those countries, the reliability of evidence is measured in terms of its source and the opposing party's ability to (cross) examine that evidence.

Verbal testimony is considered as the queen of evidence. It can be admitted only if it comes from the person who had direct knowledge of the matter he is testifying about. For instance, hearsay is a statement, other than one made by the declaring while testifying at the trial or hearing, which is offered in evidence to prove the truth of the matter asserted. Such a statement would generally be excluded from evidence. Conversely, if the statement is offered to prove something other than its truthfulness, it might be admissible.

Jurisprudence and authorities have generally considered computer printouts to be subject to the hearsay rule (when submitted for substantive purposes). In 1968, however, the British legislature issued the Civil Evidence Act. Using this
rule, a computer printout is admissible as evidence if the person testifying had direct knowledge of data and can therefore authenticate its content.

According to the Best Evidence Rule, in proving the terms of a writing, where such terms are material, the original writing must be produced, unless it is shown to be unavailable for some reason other than the serious fault of the proponent. According to the UK 1978 Interpretation Act, a computer printout is not an original.

For instance Section 7 of the Electronic Communications Act in Part II (ECA) ensures that electronic signatures and associated Certificates is admissible as evidence in legal proceedings. It is however up to the Courts to decide in a particular case on the correct use of a signature and the weight it should be given against other evidence. In this respect existing laws may preclude the use of electronic signatures or electronic writing in particular circumstances.

Imposing equivalence between traditional and electronic means of communication in one fell swoop would have unforeseen consequences in UK law. Equally, there will be cases (e.g. the registration of births, deaths and marriages) where it is not appropriate, at this stage, to allow electronic means to be used alongside traditional means.

Section 8 of the ECA, therefore gives powers to remove existing barriers on an individual basis by the amendment of existing legislation.

Part 1 of the ECA is concerned with setting up of a statutory approvals regime for bodies providing cryptographic services e.g. certificates supporting electronic signatures, to business or the public. Part 1 will not be brought into force if Industry led approvals process is successful. The Alliance for Electronic Business (AEB) tScheme has been set up to fulfil objectives. tScheme approval is based upon the profiles requesting the requirements.

15. Annex C. Time Stamping

Informative

In order to perform the validation, the certificate used by the signer at the time of the signature must be obtained, and its **validity at the time of the signature proven**. In this event, evidence must be provided that the document was signed when the certificate was valid, i.e. before the end of its validity (as indicated in the certificate validity period) and before it was revoked. Time-stamping can provide such evidence.

A time stamp by itself does not allow to know the exact time when an electronic document was signed. A time stamp is obtained by sending the hash value of the given data to the TSA. The returned time-stamp is a signed document which contains the hash value, the identity of the TSA, and the time of stamping. This proves that the given data existed *before* the time of stamping.

If the hash of a digital signature is sent to a TSA and is time-stamped before the revocation of the certificate used to generate that signature, evidence will be provided that the digital signature was formed before the revocation of the public key certificate.

If a recipient wants to hold a valid electronic signature he will have to ensure that he has obtained a valid time stamp for it, before the certificate of the signer (and any certificate involved in the initial verification) is revoked. The sooner after the signature time, the better.

There will be some delay between the time a signature is created and the time the signer's digital signature is timestamped. However, the longer this elapsed period the greater the risk of the signature being invalidated due to compromise or deliberate revocation of its corresponding certificate by the signer. Thus the signature policy should specify a maximum acceptable delay between the signing time as claimed by the signer and the time included within the timestamp.

In case of a compromission of the signer's key, the date of revocation of the signer's certificate can be compared with the date of the time stamp. If the date of the time stamp is earlier than the date of revocation, then it proves that the signature was applied before the revocation of the certificate hence the signature is valid. It also serves another purpose. Since a CA is no more responsible of taking care of the revocation of the certificates after the end of the validity period of the certificate, it is necessary to time stamp the signature to prove that is was performed before the end of the validity period of the certificate and therefore that it is based on a non-revoked certificate.

In order to avoid the need to get a timestamp prior to the signature, the purported date of the signature, as claimed by the signer, is included in the signed data. In addition it may be useful to also include a time stamp *inside* the signature. The drawback is the need to get access to a Time Stamping Authority before signing. However, this proves that the signature has been made *after* that date. Since the external time stamp indicates that the signature was made after that other date, this allows to know that the signature was performed *between* these two dates. *If* these dates are close enough, then the signature time can be reliably determined.

16. Annex D. How may a verifier really know who the signer is ?

When the signer has a name which has several homonyms (same first and family names for different persons) or uses a pseudonym there may be some ambiguities.

There is no single response to that question. This annex only gives some hints on the ways to address this issue.

Two main cases need to be considered whether or not the signer and the verifier have had some previous contact before receiving the first signed document.

16.1. Using previous contacts

This case has many variants, which are not all described.

- The signer gave his business card and the name of the CA together with the name given to him by the CA is printed on the business card.
- The signer has been using surface mails and thus has already manually signed some documents. A Qualified Certificate contains extensions that allow to include biometrics information, more exactly only the hash of the biometrics information. If the signer sends with his first signed document that biometrics information (i.e. in this case the picture of his manual signature) then the verifier can verify that it matches the hash contains in the certificate. Then the verifier can verify that the manual signatures affixed on the previously received documents looks the same as the picture of the signature attached to the document.
- The verifier has already seen the verifier in some meeting or conference and he remembers the face of the signer. A Qualified Certificate contains extensions that allow to include biometrics information, more exactly only the hash of the biometrics information. If the signer sends with his first signed document that biometrics information (i.e. in this case the picture of his face) then the verifier can verify that it matches the hash contains in the certificate. Then the verifier can verify that the picture attached with the first signed document looks the same as the face of the person seen at the meeting or conference.

16.2. Without previous contact

This case has two main variants.

- The verifier may use a company directory to get additional information about the signer which may allow to solve the ambiguity, such as: the location of his work place, his organization unit, his phone number. The company directory provides for each individual an additional entry that contains the different certificates given to the users.
- The verifier has no access to a directory (either private or public). The signer provides with his first signed document additional information about himself. This information is a subset of the registration information that was registered by the RA, at the time of initial registration or at the time of the renewal of the certificate. This signed document allows to link the name of the signer to additional attributes that the signer is willing to release to the verifier. In this way, the privacy of the signer is preserved. The additional information may be: the date of birth, the place of birth, the home address at the time of registration, titles, diplomas, etc ... This scheme has two variants:
    - The document signed by the RA is provided in electronic form, e.g. as an Attribute Certificate,
    - The document signed by the RA is provided in a paper form as a signed document.

  The later case does not provide real-time verification, unless the document manually signed by the RA is sent in advance.

17. Annex E. How does root CAs key management affect the publication of the signature policy ?

A signature policy contains the self-signed certificate of one or more root keys associated with names constraints and Certificate Policy constraints. Since the self-signed certificate contains a validity period, it is possible to know when that root key must be replaced.

There are basically two options to deal with the aspect:

- ask the signature policy issuer to re-issue a new signature policy every time one of the self-signed certificates expires, or
- create a link between a self-signed certificate referenced in the signature policy and a current self-signed certificate.

The first option is acceptable as long as the number of root keys is low (e.g. no more than 3). It must be supported as soon as any of the root keys is compromised.

The second option, which is only valid if none of the root keys has been compromised, is detailed hereafter.

RFC 2510 [CMP] describes a graceful, scheduled change-over from one non-compromised CA key pair to the next (CA key update). This allows the use of signature policies which incorporates old root keys to verify signatures issued using the new root key.

When a CA updates its key pair it must generate two extra cACertificate attribute values if certificates are made available using an X.500 directory (for a total of four: OldWithOld (i.e. the old self-signed certificate); OldWithNew (i.e. the content of the old self-signed certificate signed by the new key); NewWithOld (i.e. the content of the new self-signed certificate signed by the old key); and NewWithNew (i.e. the new self-signed certificate): OldWithNew; NewWithOld.

Verifiers using signature policies that contains expired self-signed certificates, will need access to the new CA public key protected with the old CA private key, i.e. NewWithOld.

The data structure used to protect the new and old CA public keys is a standard certificate, with no specific new extensions, hence no new data structure is required.

To change a root key, the CA operator does the following:

1. Generate a new key pair;
2. Create a certificate containing the new CA public key signed with the old private key (the "new with old" certificate);
3. Create a certificate containing the new CA public key signed with the new private key (the "new with new" certificate);
4. Publish these new certificates via a repository and/or other means.

The "new with new" certificate must have a validity period starting at the generation time of the new key pair and ending at the time by which the CA will next update its key pair.

The "new with old" certificate must have a validity period starting at the generation time of the new key pair and ending at the time by which all end entities of this CA will securely possess the new CA public key (at the latest, the expiry date of the old public key).

In this way it is possible to build a chain of certificates that consists of the self-signed certificates contained in the signature policy, and any number of tuples composed of an "NewWithOld" certificate and a new self-signed certificate.

In order for that method to be effective, "NewWithNew" and " NewWithOld" certificates must remain accessible in some repositories.

Verifiers SHALL only make use of new self-signed certificates that contain the same naming constraints. If the self-signed certificates contains naming constraints extensions, then the CA will have to re-issue such sequence of certificates for each of the naming constraints contained in the certificates.