European Electronic Signature Standardization Initiative (EESSI)

Final Report of the EESSI Expert Team

20th July 1999

Hans Nilsson, iD2 Technologies, Sweden (Project leader)
Patrick Van Eecke, ICRI-K.U.Leuven, Belgium
Manuel Medina, Univ of Catalunya, Spain
Denis Pinkas, Bull, France
Nick Pope, Security & Standards Consultancy, UK

Executive Summary

The European Commission has proposed to the European Parliament and to the Council a Directive to provide a common framework for electronic signatures. The Directive covers electronic signatures used for authentication in general as well as a particular type of "qualified" electronic signatures, which have legal equivalence to hand-written signatures. The Directive also identifies requirements that have to be met by service providers supporting electronic signatures and requirements for signers and verifiers. These requirements need to be supported by detailed standards and open specifications which also meet the requirements of European business, so that products and services supporting electronic signatures can be known to provide legally valid signatures – thus furthering the competitiveness of European business in an international market.

Under the auspices of the ICTSB, European industry and standardization bodies have launched the European Electronic Signature Standardization Initiative (EESSI). EESSI has the objective of analyzing the future needs for standardization activities in support of the European Directive on electronic signatures in a coherent manner, particularly in the business environment. An expert team appointed by EESSI has produced this report.

It should be understood that this report has been put forward with the intent of proposing standards on the basis of an open implementation framework for electronic signatures including signatures in compliance with the proposed Directive. It is not the intention of this report to establish standards that would be mandatory to support the Directive, but rather identify requirements for standards that would facilitate an open market of products and services that meet the requirements of the directive.

The most important findings of the expert team are summarized as follows:

- International standards adopted and/or developed by industry should avoid the need for detailed regulations as far as possible. A framework relating legislation and standardization is proposed in this report.
- Standards are urgently needed, and wherever possible, reference to existing recognized international standards should be preferred to the development of new standards. This report has made initial recommendations for the use of existing standards.
- Standardization requirements can be foreseen in two main areas: qualitative and procedural standards for information security and technical standards for product interoperability.
- In those cases where standards for signature products are recognized as meeting the requirements of the Directive, conformance assessment and certification could be performed by an accredited body under the European EN 45000 accreditation scheme or by a national body using equivalent criteria. A harmonized European scheme and guidelines for conformance assessment of signature products should be developed through the European co-operation for Accreditation (EA). Any standards conformance assessment scheme in this area, and the general conformance scheme against requirements of the Directive need to be aligned.
- A first set of technology-specific components should be defined that can be used to provide a technical framework for qualified electronic signatures, using asymmetric cryptography and certificate based verification, and supported by trustworthy hardware devices such as smart cards. This is needed to provide a common point of reference that is known to meet the requirements of the Directive within the shortest practical time-scale. As the market for electronic signatures develops, standardization should encompass variations and alternatives to this first set.
- For certification service providers, the following security-related standards are needed:
  - General security management codes of practice, e.g. BS7799 part 1 and part 2.

- Specification of security requirements for trustworthy systems used by CSPs. For this EESSI recommends that initially specific requirements should be placed on the cryptographic modules being used (e.g. using FIPS 140-1 or equivalent) with more general requirements based on a risk analysis. Also, a suitable protection profile based on the Common Criteria (ISO 15408) may be needed.
- A baseline Certificate Policy for service providers issuing qualified certificates. EESSI recommends that the policy is written according to the IETF PKIX framework RFC 2527 but should also include references to general security standards as described above.
- Specification of policy requirements for providers of trusted time-stamping services.

- For signature creation and verification products, the following security-related standards are needed:
  - Specification of security requirements for trustworthy hardware devices used as secure signature creation devices. For this, EESSI recommends concurrent acceptance and usage of FIPS 140-1 (or equivalent standard) and a suitable Protection Profile based on Common Criteria (ISO 15408). Although specification of a security target according to ITSEC also could be possible, the Common Criteria is preferred as it is more recent and has global recognition.
  - Specification for the creation of electronic signatures including recommendations on the user interface.
  - Specification of signature verification products and procedures.
- A number of standardization activities may be initiated and carried out by various bodies as a result of the proposals in this report. Hence, there is a strong need for technical co-ordination between these activities to ensure that a consistent standardization framework is developed.
- In the area of interoperability, the following standards are most needed:
  - Technical standard for the syntax and encoding of electronic signatures, supporting multiple signers and role signatures that are verifiable long after their initial use. EESSI recommends that this is based on a profile of and extensions to the CMS standard (RFC 2315, shortly to be replaced).
  - Profiles for PKI operational management protocols based on the Internet PKIX RFCs.
  - Profile for Qualified Certificates based on X.509.

Further details of these work areas, as well as initial proposals as to the best European or international organizations that should execute them, are given in section 8 of this report.

Finally, EESSI also proposes that:

- An " Electronic Signature Standardization Industry Advisory Group" is established in due course under the auspices of ICTSB, to give recommendations to the Commission's "Electronic Signature Committee". The Advisory Group should be composed of recognized technical experts in the area of electronic signatures from the vendor and user communities.
- An "International Electronic Signature Forum" is arranged, under the auspices of a suitable international organization, to promote and co-ordinate international activities in the area of electronic signatures.
- Interoperability trials between suppliers of electronic signature products and services should be encouraged to promote the implementation of interoperable solutions.

Table of contents

1. Introduction

1.1 Background

The development and use of authentication products and services is still in its introductory stage. Systems exist which use authentication for commerce, administration and public services; however, there is no complete set of agreed industry standards or technical specifications for their use. Without such standards it is not considered possible to provide a common level of security which can be recognized as being valid for use at regional level, even less at international level.

The Communication of the European Commission " A European Initiative in Electronic Commerce" identified the need for electronic signatures as a key issue for electronic commerce. Whilst the signing of contractual exchanges for electronic commerce are not the sole application of electronic signatures it is likely to become an essential component for the future of European business in the competitive global market.

At the request of the Council, the European Commission has proposed a Directive [1] to provide a common framework for electronic signatures. It is not the intent of this Directive to cover the whole domain of applications of authentication, but rather to focus on the legal validity of an electronic signature attached to an electronic document so that it has the same legal effect as a hand written signature attached to a paper document. However, contractual freedom should prevail for "electronic signatures used within closed groups, for example, where contractual relationships already exist". The Directive identifies minimal requirements for trusted service providers supporting electronic signatures as well as requirements for signers and verifiers. These requirements need to be supported by detailed standards and open specifications which are recognized as meeting these requirements so that products and services supporting electronic signatures can be known to provide legally valid signatures.

Several standardization initiatives have already been launched in this area at the national, regional and international levels by organizations and industry fora. Worth to mention are the activities of the International Chamber of Commerce, the UNCITRAL activity on Model Law, the ILPF current inventory, the IETF and ABA standardization activities. They are, however, at this stage, not necessarily sufficient to provide a harmonized legal framework for Europe. A consistent and coherent approach is necessary, overseen by the "Electronic Signature Committee" (as identified in Article 9 of the Directive), so that the legal framework for electronic signatures can build, as far as possible, upon standards and other forms of voluntary agreements. Such agreements can be used to provide signatures which can be recognized as legally valid not only across Europe, but at international level.

In order to provide timely standards permitting full and efficient implementation of a common framework, based on consistent Member States' legislation, standardization initiatives should be encouraged at an early stage, in particular so as to obtain adequate international co-operation.

1.2 The mandate from the Commission

Industry and European standardization bodies, within the framework of the ICTSB, have been requested by the Commission to analyze the future needs for standardization activities to support the essential minimum legal requirements as stated in the Directive in relation to electronic signatures products and services available on the market. The assessment of available standards and current initiatives at global and regional level, both in formal standardization bodies and industry consortia, should identify gaps and the need for any additional standardization initiatives in all relevant forms, such as standards, specifications, agreements, workshops or any other form

1 This report references the Common Position of the "Proposal for a Directive of the European Parliament and of the Council on a common framework for electronic signatures" dated 24th June 1999.

of consensus building. On the basis of this analysis, an indicative work programme should be proposed.

Industry and European Standardization bodies should set up an implementation framework, compliant with the minimal legal framework stated by the Directive. This will answer business needs and bring the full advantage of the legal recognition of the electronic signature in support of the development of the open electronic commerce environment.

1.3 The European Electronic Signature Standardization Initiative (EESSI)

To meet the requirements of the Commission mandate, the ICTSB has launched the European Electronic Signature Standardization Initiative (EESSI) placed under the direction of a steering group composed of:

- Industry representatives, members of associations such as HLSG (High Level Strategy Group for ICT Standardization) and EEMA;
- ICTSB member organization representatives with an interest;
- Observers from the European Commission;
- Industry experts.

The Steering Group is assisted in its work by an Expert Team with the following members:

Hans Nilsson, ID2 Technologies, Sweden (Project leader)
Patrick Van Eecke, ICRI-K.U.Leuven, Belgium (Legal Expert)
Manuel Medina, Univ. Polit. of Catalunya, Spain
Denis Pinkas, Bull, France
Nick Pope, Security & Standards Consultancy, UK

In addition, a review team has been appointed consisting of:

Leslie Seymour, consultant
Bart Preneel, COSIC, K.U.Leuven, Belgium
Robert Willmott, consultant, UK

1.4 The task of the Expert Team

The expert team has been requested to produce a report as the starting point for the steering group to meet the EESSI objectives. The report should prepare the grounds for the necessary standardization activities and identification of the standardization needs in support of the emerging legal framework for electronic signatures in the European Union, based on an assessment of existing standards and technical specifications in this area.

The expert team should provide an analysis and evaluation of the role of standardization in response to essential legal requirements as they are currently under discussion (based on the proposed Directive) or already adopted by Member States.

The legal requirements set out in the proposed Directive focus on certificates and certification services to ensure minimum levels of security and to allow their free movement throughout the Single market. Standardization efforts should therefore be oriented towards establishing transparent, proportionate and non-discriminatory rules for such certification schemes.

In addition to certificates and certification services covered by the scope of the proposed Directive, standardization activities should also cover the off-line use of electronic signatures and electronic signature products and services to be made available to the end-user.

It is not the intention of this report to establish standards that would be mandatory to support the Directive, but rather identify requirements for standards that would facilitate an open market of products and services that meets the requirements of the directive.

The requirements have to be considered in an open environment, and in close co-operation with all relevant parties; subsequently adequate and efficient co-operation mechanisms should be put in place in view of establishing international-wide consensus among all parties concerned.

Arrangements should be proposed to establish the relevant international co-operation to ensure that the relevant standards are available at global level.

The expert team was asked to include the following specific items in the report:

- An inventory of existing technical work, including:
  - pilot projects at national level;
  - European projects (including standardization, RTD-related work);
  - International work (e.g. ICC and in standards bodies and consortia);
- Itemisation of standardization and other relevant requirements (from the EU Directive and also from other sources such as the HLSG report), including:
  - technical infrastructure work;
  - legal work and service aspects (of various applications) requiring management standards, codes of practice, guidelines etc.;
- Definition of a Work Programme that meets these requirements and that does not duplicate work taking place elsewhere.
- Work repartition – what, where and how? Recommended time-scales for deliverables.
- A proposed programme for the creation of European and international visibility of the above.

The expert team was not asked to include a survey of existing and proposed legislation, since this recently has been covered extensively in the report «Legal Aspects of Digital Signatures», prepared for the European Commission by ICRI-K.U.Leuven.

2 Business and user requirements

2.1 Various uses of electronic signatures

The document "COM (97)503 - Ensuring Security and Trust in Electronic Communication" lists various uses of electronic signatures:

- electronic signatures used for official communication with public institutions (e.g. calls for tender, exchange of application forms, identity documents, tax declarations, transmission of legal documents);
- electronic signatures used for contractual relations in open networks (e.g. electronic buying and selling, financial transactions);
- electronic signatures used in closed systems (e.g. a corporate Intranet);
- electronic signatures used for personal purposes;
- electronic signatures used only for identification or authorization purposes (to verify the identity of a correspondent or of his specific attributes e.g. an authorisation to log into a computer system, identification of Web servers).

For the two first areas above, it is envisaged that the electronic signature is used with equivalent legal effect as a hand-written signature.

For the three last areas, the requirement is only for authentication. Those uses do not imply legal binding proof, either because of the nature of the application (limitation to authentication purposes) or of the nature of the environment (Intranet, personal purposes). In that sense, the full use of «legal» electronic signature is not relevant.

Note: At this time there exist several concurrent definitions of the term "electronic signature". As a result this term is used in various communities with different meanings. The most internationally recognized definition has been proposed by UNCITRAL. There exists an internationally recognized definition of "digital signature" (ISO 7498-2. see annex B for the full definition) which is too often used interchangeably with the term "electronic signature". It defines a security *mechanism* which can be used to build various security *services* such as authentication, data origin authentication, data integrity, or non-repudiation.

2.2 A business scenario using electronic signatures

A business scenario is proposed to help consider the requirements. The business scenario consists of three stages of business transactions:

a) Pre-contract exchanges

b) Contract establishment

c) Post-contract establishment

Pre-contract exchanges could include, for example, requests for product and pricing information, discussion of possible contract terms etc. During this stage no commitments are entered into. There is a requirement not to mislead but this only requires simple evidential consideration. Thus, at this stage, there is a requirement for data origin authentication, but not for indication of intent.

Contract establishment could include, for example, a specific offer of contractual terms and acceptance of those terms. This requires clear evidence of intent from an identifiable source. Thus, at this stage there is a requirement for an electronic signature that serves as evidence of the origin of data and that the originator had a clear intent related to that data. During the exchange of contract, the time between creating a signature and the relying party verifying the signature will be relatively short.

In the case of later dispute between a signer of contractual conditions and the other party relying on those conditions, the data together with its electronic signature would be presented as evidence by the relying party to be verified by some arbitrator or judge. This can occur a significant period (e.g. years) after the electronic signature was created.

Post contract exchanges involve further exchanges under the terms of the contract (e.g. making a specific order within general terms defined in the pre-agreed contract). In general the requirements for protecting the exchanges will be dependent on the application covered by the contract.

EESSI requirement*: The further development of internationally recognised business scenarios, as part of the development of standards for electronic signatures, would significantly aid the understanding of the requirements.*

2.3 Requirements for the business community

On February 24, 1999, the EESSI project arranged a consultation meeting to discuss the requirements for electronic signature standardization with the business community, users, regulators, service providers, product suppliers and various standards bodies. The following list summarizes the most urgent needs and viewpoints expressed at the meeting:

- Although the Directive aims to be technology neutral, there is an urgent for at least one standardized technical solution that can meet mass-market requirements. It was generally stated that public key technology is currently the favoured market choice.
- There are urgent and important standardization requirements for signature format, certificate and CRL format profiling, certificate verification and cross certification processes and time-stamping services.
- There is also a need for interoperability standards for signed documents and signed files, and for signature creation and verification devices.
- There is often a need to put more than one electronic signature on the same document.
- There is a strong user requirement for ease of use of components and services, as well as compatibility of user hardware and software.
- Privacy issues (personal data protection) must always be taken into account.
- There is a need for security and quality standards for the assessment of the «trust» that can be held in service providers in this area. However, trust is not just «technical security»; there is also a need for the organization to be assessed and trusted.
- There is need for standardized procedures and means to access revocation information, both in the short and the long term.
- The issue of long-term validation of electronic signatures in archives needs further studies and guidelines.

Currently, several countries in Europe are already either specifying or deploying solutions for electronic signatures. Some countries are issuing or planning to issue «electronic identity cards» with private keys and certificates to its citizens. These cards are to be used for authentication and electronic signature purposes, both for official communication with public institutions and for business-to-consumer applications.

Also, several European banks have already deployed, or are planning the deployment of electronic identity cards to their customers, both for home banking, corporate banking and electronic commerce. A number of very large European and international banks are planning such a deployment through the establishment of Identrus (formerly called Global Trust).

Because of all these current activities, the business community has a very urgent need for standardization in the area of electronic signatures. If standards are not set quickly enough, different countries and business communities will end up specifying and deploying incompatible solutions, which will seriously hamper the development of a European market for electronic commerce.

3. Implications of the Directive for Standardization

In order to fulfil its task and draw up a work programme, the EESSI project has necessarily analysed the implications of the Directive[2] from the perspective of industry and the standardization community. This analysis is not a formal legal interpretation of the Directive, but constitutes the expert team's understanding of the present content. It does not represent the position of the European Commission.

It should be understood that this report has been put forward with the intent to propose standards on the basis of an open implementation framework for electronic signatures including signatures in compliance with the proposed Directive.

On 13 May 1998, the European Commission submitted a proposal for a European Parliament and Council Directive on a common framework for electronic signatures (COM (1998) 297 final, O.J. 23 September 1998, C 325/04-11).

The proposed directive is based on article 47 (2) concerning the freedom of establishment, article 55 on the freedom to provide services and article 95 relating to approximation of laws, of the Treaty of Amsterdam. The legislative procedure laid down in article 251 of the Treaty is being followed.

On 22 April 1999 the Council of Ministers on its meeting held in Luxembourg agreed on a Common Position, which contains a number of changes compared with the original draft of 13 May 1998. An adoption of the Common Position by the European Parliament is soon to be expected.

The Commission's proposal aims at ensuring the proper functioning of the internal market in the field of electronic signatures by creating a harmonised and appropriate legal framework for their use. The proposal is based essentially on the following principles:

1. ensuring technological neutrality. Although the proposal concentrates on digital signature technologies employing public-key certificate-based cryptography, it aims to be technology-neutral and therefore does not focus only on those kinds of signatures;
2. avoiding any prior authorization scheme for the provision of CSPs so as not to limit the supply of such services and technological innovation, whilst permitting the introduction of voluntary accreditation schemes for providers of such services with the aim of providing confidence in the security level ;
3. recognising the legal validity of an electronic signature, by preventing it from being denied validity solely on the grounds that it is in the form of electronic data, and guaranteeing that it is considered equivalent to a hand-written signature if it meets a certain number of conditions.

A few definitions in the Directive differ from the terms used in existing technical standards. Since this report concerns standardization, we would like to make the following clarifications:

Definition in the Directive	Term used in this report	Explanation
Certification Service Provider (CSP)	CSP	In the Directive, this definition encompasses not only certification authorities (CAs), but also time-stamping authorities, directory service providers and «any other service provider related to electronic signature». It is thus included in the previously popular ISO defined term Trusted Third Party

2 This report references the Common Position of the "Proposal for a Directive of the European Parliament and of the Council on a common framework for electronic signatures" dated 24th June 1999.

		(TTP). Since the term «Certification service provider» easily may be confused with CA, we have chosen to always use the abbreviation CSP, keeping in mind that it actually encompasses a range of service providers. Whenever we need to talk specifically about CAs, we will either use the term CA, or the equivalent term «CSP issuing certificates».
Accreditation	Accreditation/ Certification	In relation to standards, the term accreditation means assessment and approval of Certification Bodies (as described in ISO/EN 45010). The term certification is generally used when a "Certification Body" certifies that an organization or product conforms to a standard. Whilst, as described later, accreditation may be applied directly to CSPs, checking conformance of products and CSPs against a standard is generally considered to be more akin to certification. To clearly separate out accreditation and certification, the separate terms are used in this report.
Signatures fulfilling the requirements of article 5.1.	Qualified electronic signature	A term is needed for electronic signatures meeting the requirement identified in 5.1 of the Directive, which includes requirements for advanced electronic signatures, qualified certificates and secure electronic signature creation devices. For the purpose of this report, we have introduced the term «qualified electronic signature».
(Not used in the Directive)	Signature Policy	A named set of rules for the creation and verification an electronic signature, including any use of CSPs, that is recognized as being valid within a given legal / contractual context.
ditto	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. (Many of the requirements of a signature policy will be met by the rules in a certificate policy.)
ditto	Certification Practice Statements (CPS)	A statement of the practices which a certification authority employs in issuing certificates.

Annex B contains a list of other important standards and definitions in the area of electronic signatures.

3.1 The scope of the Directive

Article 1 describes the scope of the Directive. The Directive aims both at facilitating the use of electronic signatures as well as contributing to their legal recognition. Therefore, it establishes a legal framework for electronic signatures, signature products and certain certification services in order to ensure the proper functioning of the internal market.

Certification Service Providers (CSPs) and electronic signature products

The Directive aims to cover every kind of service related to electronic signatures. The Directive explicitly states in its recitals that CSPs should not be limited to the issuance and management of certificates, but also encompass any other service using or ancillary to electronic signatures, and thus covers all of the following services:

- Certificate issuing

- Registration services
- Directory services
- Time-stamping services

... as well as:

- Computing services
- Consultancy related to electronic signatures.

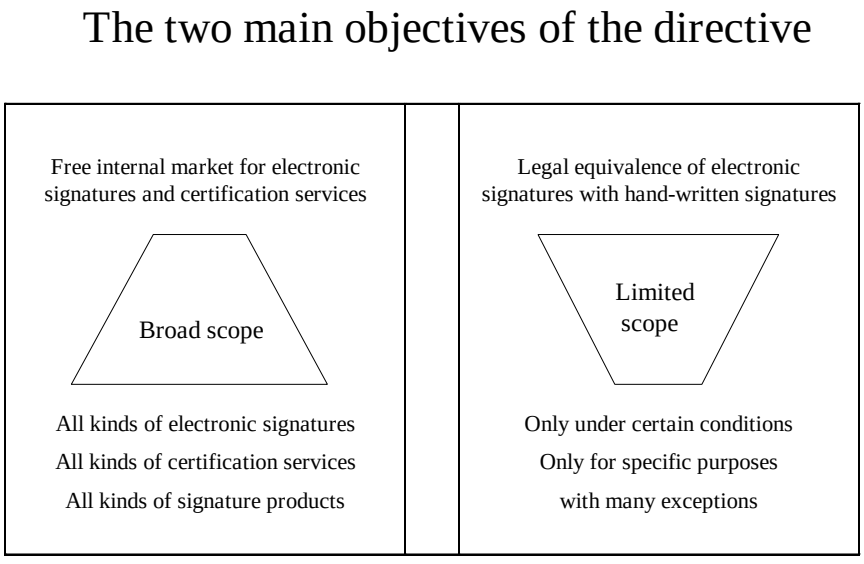
The Directive also aims to ensure a free flow of electronic signature products in the Internal Market through the publication of recognized standards for such products.

Electronic signatures

For the legal effect of electronic signatures, however, the Directive has a limited scope:

- The Directive does not cover aspects relating to the conclusion and validity of contracts or other legal obligations where there are formal requirements prescribed by national or community law.
- It does not affect rules and limits governing the use of documents contained in national or community law.
- Parties are still free to agree among themselves the terms and conditions under which they accept electronically signed data (to the extent allowed by national law).

The Directive, in other words, chooses for a broad approach when guaranteeing a free market for CSPs but for a limited approach when giving legal effect to electronic signatures.



3.2 Definitions

Article 2 of the Directive contains a few definitions. These definitions are only used in a Directive related environment and do not necessarily correspond to technological terminology.

3.2.1 The signature definition

For the purpose of this Directive:

1.”electronic signature” means data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication.

1a. "advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory ;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

2. “signatory” means a person who holds a signature creation device and acts either on their own behalf or on the behalf of the person or the entity they represent.

It is noteworthy that the term “digital signature” is not used.

In the light of the Commission's strategy to encompass as many services and products and electronic signatures in the scope of application of the Directive (for the sake of free circulation and the non-discrimination of electronic signatures) a very broad definition of electronic signatures is used.

The technology neutral approach of the Directive would not allow reference to specific technologies, such as digital signatures based on asymmetric cryptography. However, it is clear that the Directive, when describing an "advanced electronic signature", has taken into consideration the characteristics of asymmetric cryptography and certificate-based verification.

The use of the term “signature” in the Directive may cause confusion and may provoke a limited approach, suggesting that the directive would only cover electronic alternatives for the well-known hand-written signature. This is not true. Instead, the Directive uses a distinction between ”electronic signature ” and ”advanced electronic signature ”.

An "**electronic signature**" without being further qualified, is indeed an *electronic authentication*. The term ” authentication ” itself is not defined nor explained in the recitals of the Directive and thus leaves room for a broad interpretation. However, the term is usually defined as ”validation of a claimed identity”. Every type of electronic authentication will be regarded as an electronic signature, as long as it is attached to or associated in a logical way with other electronic data. Thus, biometric authentication methods, such as Penop™ or Smartpen™, are regarded as electronic signatures, Message Authentication Codes (MAC), which are based on symmetric cryptography, are electronic signatures. Public key authentication schemes, such as digital signatures, are electronic signatures. The definition of an electronic signature in the directive does even not exclude the typed name at the bottom of an email or the attachment of a scanned signature to a document.

All kinds of authentication which are currently being used in a paper environment (e.g. a stamp or a seal) and which can be replaced by electronic means fall under the scope of the directive. As such, the directive has taken a much more general approach than other legal instruments or guidelines dealing with electronic signatures.

When defining an “**advanced electronic signature**”, the Directive’s definition is similar to the digital signature as defined by ISO 7498-2 (see Annex B), which also is technology neutral. Digital signatures as defined by ISO may be realized in practice not only using asymmetric cryptography but also using symmetric cryptography associated with tamper-proof signature creation devices and tamper proof signature verification devices. In the same way “advanced electronic signatures” can be realized using either technology. An "advanced electronic signature" without being further qualified, is indeed equivalent to a “digital signature”, as defined by ISO.

Contrary to some other existing legal instruments and guidelines (E.g. UNICTRAL, some U.S. laws) the Directive does not consider the approval of the contents by the signatory as an essential element of an electronic signature. The Directive accepts every electronic authentication method as an electronic signature, whether it invokes legal effect or not, and whether the signatory approves the contents of the document or not. By taking this broad approach the directive is able to cover every kind of authentication without having to tackle the legal differences which are existent between the European Member States' legal systems. The signatory's approval thus needs to be specified by other means, for example in the text of the signed document, or by referring to a "signature policy" which includes approval.

The Directive uses the term "person" in its definition of signatory, and does not explicitly state "natural persons" as in other directives. Thus, the Directive currently leaves it to the Member States to decide if an electronic signature should be limited to natural persons or also include legal persons, in accordance with national legislation with regard to validity and effect of signatures.

3.2.2 Other definitions

A **certification service provider** (CSP) means a person who or entity which issues certificates or provides other services related to electronic signatures.

The typical Certification Authority (CA) in a PKI (Public key infrastructure) environment is certainly regarded as a CSP, but also registration authorities, time-stamping service providers, electronic notaries, electronic archiving service providers are CSPs in the sense of the Directive as long as there exists a link with electronic signatures.

An **electronic signature product** means hardware or software, or relevant components thereof, which are intended to be used by a certification service provider (CSP) for the provision of electronic signature services or used for the creation or verification of electronic signatures.

In defining an electronic signature product, the Directive has also taken a broad approach; smart cards for the storage of private signature keys, an electronic signature program, such as the ones embedded in the Microsoft Internet Explorer™ or Netscape Navigator™ and its related electronic mail programs, biometric devices to give access to a signing function: all are regarded as electronic signature products.

Signature creation data means unique data such as codes or private cryptographic keys, which is used by the signatory in creating an electronic signature.

A signature creation device means a configured software or hardware device to implement the signature creation data.

Signature verification data and a signature verification device is *mutatus mutandis* defined in the same manner. A smart card functioning not only to store private signature keys but also to sign effectively would be a typical example of a signature creation device. If this device meets the specific security requirements, which are contained in Annex III of the Directive, it will be regarded as a **secure signature creation device**.

A **certificate** means a digital attestation which links a signature verification device to a person, and confirms the identity of that person.

The ISO-ITU standardized X.509 certificates for public key authentication can certainly be regarded as certificates in the sense of the Directive.

A **qualified certificate** means a certificate which meets the requirements laid down in Annex I and is provided by a certification service provider (CSP) that fulfils the requirements laid down in Annex II.

Qualified certificates are only relevant in relation to the legal recognition of electronic signatures under the conditions of article 5.1 of the Directive (see section 3.4 below), and in relation to liability of CSPs issuing qualified certificates to the public (see section 3.6 below).

3.3 Internal market and market access principles

The principles of the Internal Market are dealt with in article 4 of the Directive. As regards to certification services (including all services provided by CSPs), it states that a Member State shall only apply to national legislation that conforms with the Directive to CSPs established on its territory. Member States may not restrict the provision of services from CSPs that originate in another Member State either. Article 4 also obliges the Member States to ensure that electronic signature products complying with the Directive shall be permitted to circulate freely in the Internal Market.

Furthermore, article 3 of the Directive describes the market access principle relating to certification services and products for electronic signatures.

Certification Service Provider

For the provision of certification service the Directive sees four market access principles:

1. Member States may not make the provision of certification services subject to prior authorization (mandatory licensing). Prior authorization does not only mean any permission which requires the CSP concerned to obtain a decision by national authorities before being allowed to provide its services, but also any other measures having the same effect;

2. Member States may, however, introduce or maintain voluntary accreditation schemes to encourage enhanced level of services and best practice among CSPs. The Directive defines voluntary accreditation as:
   "any permission, setting out rights and obligations specific to the provision of services, to be granted upon request by the CSP concerned, by the public or private authority charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the CSP is not entitled to exercise the rights stemming from the permission until it has received the decision by the authority".
   However, the conditions relating to the accreditation must be objective, transparent, proportionate and non-discriminatory. Furthermore, Member States may not limit the number of accredited CSP. (It should be noted that the term "Accreditation" used by the Directive should be read as " Certification" in standardization terminology. The term "Accreditation" in the conformance assessment area is reserved for the assignment of specific bodies (mostly laboratories) to certify services or products.

3. Member States shall ensure the establishment of a supervisory system to control the CSP established on its territory issuing qualified certificates to the public. CSP willing to issue such qualified certificates will have to meet the conditions of Annex II of the Directive. Such "a posteriori supervision" may either be governmental or operated by the private sector.

4. With respect to the use of electronic signatures in the public sector, Member States are allowed to make CSPs and products subject to additional requirements if these requirements are objective, transparent, proportionate and non-discriminatory, and only relate to the specific characteristics of the application concerned. Typical examples are additional requirements in the field of social security or taxation.

The following table summarizes the controlling instruments for CSPs mentioned in the directive:

Controlling instrument	Characteristics	Description	Status in the Directive
Authorization	- Obligatory - A priori	CSP is not allowed to provide any service without a prior permission	Forbidden
Accreditation/ Certification	- Voluntary - A priori	CSP gets a quality label if it proves it meets certain requirements	Not mandatory. Allowed if conditions are objective, transparent, proportionate and non-discriminatory and without numeric restrictions

Special cases

CSP issuing qualified certificates to the public	Obligation for Member States to control via supervision: - E.g. self-declaration scheme with subsequent control by governmental body or private institution
CSP issuing certificates for public sector purposes	Member State is allowed to set up additional requirements and to control it via - accreditation scheme - self-declaration scheme

Signature products

For signature products, Member States are obliged to ensure that electronic signature products complying with the Directive can circulate freely in the Internal Market.

Regarding the security of the signature products, the Commission will establish and publish reference numbers of generally recognised standards for electronic signature products in the Official Journal. A product complying with a recognised standard will be presumed to meet the security requirements of the signature products used by the CSP (= point (f) of Annex II) and of the secure signature creation devices (=Annex III).

Conformity of secure signature creation devices with Annex III must be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States in determining whether such a "notified body" is appropriate to be designated. Determination of conformity with the requirements of Annex III made by these bodies shall be recognised by all Member States.

It is currently unclear how conformance assessment of trustworthy systems (Annex IIe) shall be performed, since this is not mentioned in article 3.4 of the Directive. However, it can be assumed that this also should be performed by appropriate public or private bodies, similarly to secure signature creation devices.

No specific controlling mechanisms are mandated for signature verification products. However, Member States and Commission are requested to work together to promote development and use of

signature verification products, in the light of the recommendations in Annex IV and in the interest of the consumer.

3.4 Legal recognition

5.1	Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature creation device (a) satisfy the legal requirement of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies that requirement in relation to paper-based data, and (b) are admissible as evidence in legal proceedings.
5.2	Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that the signature is in electronic form, or is not based upon a qualified certificate, or is not based upon a qualified certificate issued by accredited certification service provider, or is not created by a secure signature creation device".

Article 5 is a core element in the Directive. This article describes the possible legal effects of an electronic signature in the Internal Market.

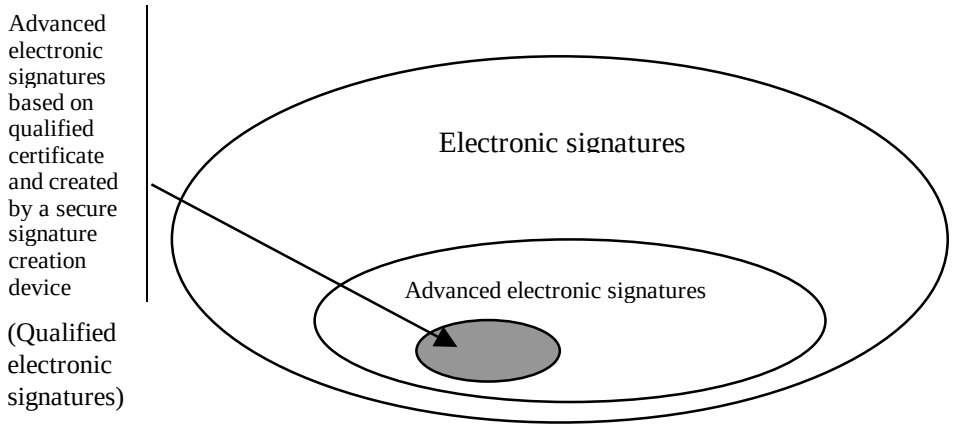
As a general principle the Directive states in article 5.2 that Member States may not deny the legal effect of an electronic signature or the admissibility as evidence in legal proceedings only because of the electronic form of the signature or because the requirements of the Annexes I to III are not being fulfilled.

Hence, this general acceptance rule of electronic signatures means that Member States may not draft or maintain legislation forbidding the use of electronic signature and authentication tools for legal purposes solely on the grounds that they are in electronic form. This does not effect national rules regarding the free consideration of evidence by the judge.

A second principle of the Directive is that Member States are obliged to recognize certain types of electronic signatures with the same legal effect as it would give to hand-written signatures (article 5.1).

This extra guarantee would only be valid for electronic signatures fulfilling certain technical security requirements: only ”advanced” electronic signatures which are based on a ”qualified” certificate and which are created by a ”secure” signature creation device have this advantage. Member States shall ensure that this type of electronic signature satisfies the legal requirement of a signature in relation to data in electronic form in the same way as a hand-written signature satisfies the requirement in relation to paper-based data. These signatures shall also be admissible as evidence in legal proceedings.

The conditions for meeting the technical minimum requirements can be found in the definition of an ‘advanced electronic signature’ and in the Annexes I, II and III of the Directive. Although not defined in the Directive, this type of electronic signature could be called a “**qualified electronic signature**”.



Article 5 thus provides two levels of legal certainty for electronic signatures depending on the level of technical security related to that electronic signature. On a first level, electronic signatures in general, cannot be denied legal effect. On the second level, electronic signatures fulfilling some minimal technical security requirements will have the same legal effect as hand-written signatures.

In some cases and for some applications, the technical security functions required by the Directive may not be sufficient. In those cases, additional technical requirements, such as time-stamping, may be introduced by product and service developers to *enhance* the technical security of all types of electronic signatures, including qualified electronic signatures.

3.5 The annexes

The annexes constitute an important part of the Directive. Nevertheless, with the exception of Annex IV, they are only relevant for the use of electronic signatures as legal alternatives for hand-written signatures, i.e. in relation to article 5.1 of the Directive. The applicability of the liability rules (article 6) and the foreign recognition rules (article 7) of the Directive is also only restricted to this context.

Annex I

The obligations contained in Annex I relating to the qualified certificate are purely requirements for the contents of the certificate. A certificate must at least contain the information referred to in Annex I in order to be a candidate for being a qualified certificate.

It is expected that an X.509 version 3 certificate making use of the appropriate extensions, will be able to contain the necessary information.

The Directive aims to ensure that a party relying upon an electronic signature based on a qualified certificate can determine all of the information specified in Annex I on the basis of the certificate only. This implies that either all this information is fully available in the certificate itself, or that it is present in an encoded form which is interpreted by all electronic signature products in a uniform, standardised way when presented to the relying party (for example a code in the certificate and a standardised full text linked to this code in the product). Incorporation by reference, for example by referencing a URL, is not acceptable, because the information on this URL can change without notice.

It should be noted though that a certificate containing the obligatory elements of Annex I will be regarded as a qualified certificate only if it has been issued by a certificate service provider complying with the obligations of Annex II.

Annex II

Articles 2.(10) and 2.(11) of the Directive imply that CSPs issuing qualified certificates must fulfil at least the technical and organizational security requirements laid down in Annex II. Only a CSP meeting the requirements of Annex II is able to issue qualified certificates. Moreover, CSPs

fulfilling Annex II requirements and issuing qualified certificates to the public will be subject to the specific liability system as described in article 6 of the Directive.

The Annex states that a CSP that issues qualified certificates must for example ensure the operation of a prompt and reliable certificate directory and secure and immediate revocation service (e.g. CRL or certificate revocation list in PKI terms).

A CSP also has to verify the identity and if applicable any specific attributes of the person to which a qualified certificate is issued by appropriate means in accordance with national law. It also has to ensure that the date and time, when a certificate is issued or revoked, can be determined.

Noteworthy is that a CSP is also obliged to inform the person applying for a certificate of the precise terms and conditions for the use of the certificate, including any limitations on the use of the certificate, the existence of a voluntary accreditation and the procedures for complaints and dispute settlement.

Annex III

Annex III states the requirements that signature creation devices have to fulfil in order to be regarded as a secure signature device. Electronic signatures created by a secure signature device and supported by a qualified certificate would get the legal recognition following the specifications of article 5.1 of the Directive.

A secure signature creation device must at least ensure by appropriate technical and procedural means that:

- the signature creation data used for signature generation can practically occur only once, and that its secrecy is reasonably assured. The exact interpretation of this requirement is open to debate (see section 6.1.1).
- the signature creation data used for signature generation cannot be derived with reasonable assurance and that the signature is protected against forgery using currently available technology. In digital signature terms, this requirement would mean that it should not be possible to recreate the private key by for example deriving it from the public key.
- the signature creation data used for signature generation can be reliably protected by the legitimate holder against the use of others. The use of a smart card or other hardware token for storing the signature creation data (e.g. private key) may be expected to fulfil this requirement.

Interesting is that the words ‘reasonably’ and ‘reliably’ are not defined nor explained which thus leaves room open for interpretation. A last requirement for a signature creation device to be deemed to be secure is that it must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process. A secure signature creation device thus, in itself, does for example, not have to provide the functionality of showing the signatory what he is to sign (the so-called WYSIWYS, or what-you-see-is-what-you-sign-technology), but should not make it impossible to utilize technology allowing the signatory to see what he signs. It can be assumed that currently no existing signature devices prevent the implementation of this functionality.

Annex IV

Annex IV contains a few recommendations for the verification of electronic signatures. **This annex applies to all electronic signatures, and is the only one that is not obligatory to fulfil for qualified electronic signatures (with legal effect according to article 5.1).**

The term ‘displayed’ in the text of Annex IV should be read in a broad sense and does not only mean the display of the data on a screen, but also every other functionality of presenting the signed information to the verifier: text, voice, images etc.

The Annex advises that during the signature verification process, it should be ensured with reasonable certainty, that:

- The data used for verifying the signature correspond to the data presented to the verifier, and that the signature is reliably verified and the result of that verification is correctly presented.
- The verifier can, as necessary, reliably establish the contents of the signed data.
- The authenticity and validity of the certificate required at the time of signature verification are reliably verified, that the result of verification and the signatory's identity are correctly presented and the use of a pseudonym is clearly indicated; and
- Any security relevant changes can be detected. This last requirement could mean that in case of failed verification, the verifier is made aware of it by, for example, an indication ”failure to verify”.

Noteworthy is that the Annex IV recommendations are not restricted to specifications for signature verification devices only but to the signature verification process as a whole.

3.6 Liability

A minimum liability regime for CSPs is established in article 6 of the Directive. **This liability regime only applies to CSPs issuing qualified certificates to the public.**

Member States are obliged to make sure that a CSP issuing certificates to the public is liable for damage caused to any person who reasonably relies on the certificate.

The CSP would, unless he proves that he has not acted negligently, be liable for:

- inaccuracy of the contents of the qualified certificate at the moment of issuance,
- non-functioning together in a complementary manner of the signature creation device and signature verification device when the CSP provides the signature devices,
- the non-assurance that at the time of the issuance of the certificate, the person identified in the qualified certificate held the signature creation data corresponding to the signature verification data given or identified in the certificate, and
- failure to register revocation of the certificate.

The Directive, however, limits the liability of CSPs by obliging the Member States to ensure that CSPs may indicate limits on the uses of the certificates and on the value of transactions for which the certificate can be used. The limits must, however, be recognisable to third parties. The CSP shall not be liable for damages arising from a contrary use of a qualified certificate, which includes limits on its uses.

Liability regime: Only for CSP in the sense of Annex II, issuing certificates to the public in the sense of Annex I.

<table>
<tr><th>Liability causes</th><th>Exemptions</th></tr>
<tr><td>Incorrect contents of the certificate</td><td rowspan="4">CSP can prove he has not acted negligently

Certificate is used contrary to the limits of the certificate</td></tr>
<tr><td>Person identified in certificate does not hold corresponding signature creation data</td></tr>
<tr><td>Incorrect matching of signature creation and verification data (if CSP provides these data)</td></tr>
<tr><td>Malfunctioning of the CRL</td></tr>
</table>

3.7 Third countries

Article 7 covers the international aspects of the Directive and is also restricted to the issuance of qualified certificates.

Certificates issued to the public as qualified certificates by a foreign CSP (i.e. established outside the European Community), may be recognised as qualified certificates within the European Community in three situations:

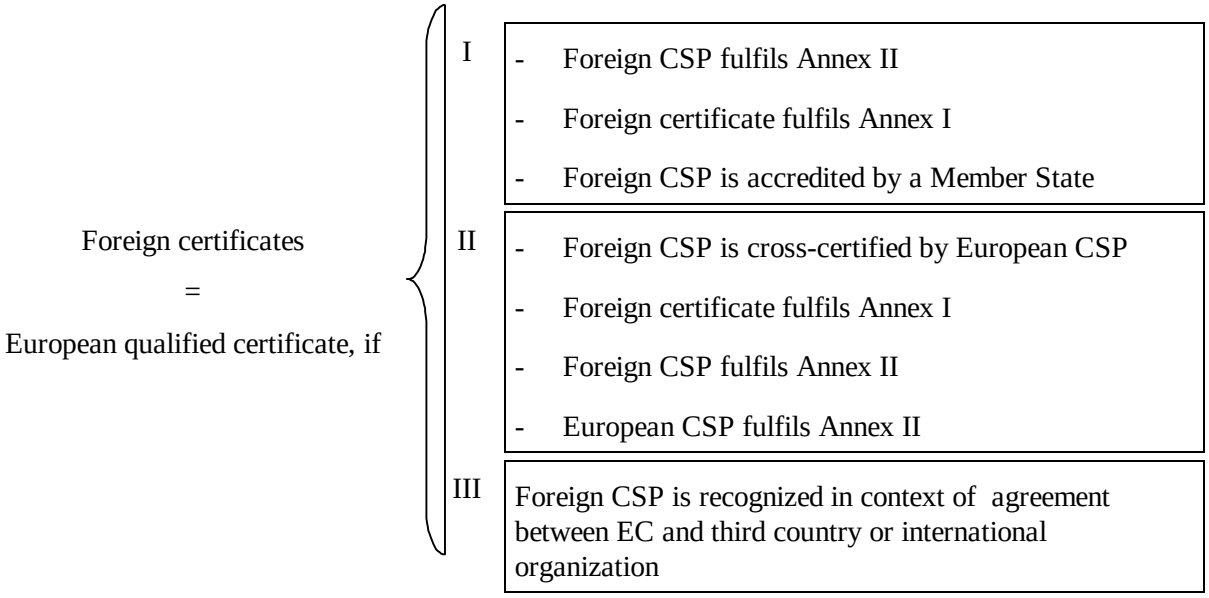
a) the issuer in the third country meets the requirements of the Directive and is accredited by a Member State in the context of a voluntary accreditation scheme,

b) the foreign certificate is guaranteed by a European Community CSP fulfilling the requirements of the Directive, and

c) the certificate or the CSP is recognised in the context of a bilateral or multilateral agreement between the European Community and third countries or international organizations.

Article 7 also gives the European Commission the task of making proposals to implement standards and international agreements for facilitating cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries.

Three ways for equivalency between foreign certificates and qualified certificates in Article 7:



3.8 Data protection

Data protection rules are incorporated in article 8 of the Directive. The general Data Protection Directive 95/46/EC applies to CSPs and national bodies responsible for accreditation or supervision.

Furthermore, CSPs issuing certificates to the public may collect personal data only **directly** from, or with the explicit consent of, the data subject. Also important is the fact that Member States may not prevent CSPs inserting a **pseudonym** in the certificate instead of the signatory's name.

3.9 The Electronic Signature Committee

An advisory "Electronic Signature Committee", composed of the representatives of the Member States and chaired by a representative of the Commission, assists the European Commission.

The Electronic Signature Committee is to be consulted for:

- Clarifying the requirements of the annexes;
- Establishing the criteria for the designation of national bodies which determine the conformity of secure signature creation devices with Annex III (see Article 3.4);
- Determining the generally recognised standards for electronic signature products which would comply with the requirements laid down in point (f) of Annex II and Annex III (see Article 3.5). Reference numbers of these standards will be published by the Commission in the Official Journal.

It is currently unclear what is meant by “generally recognised standards” in this context. Within the standards community, the term “standards” and “publicly available specifications” is generally used, and we assume that this proposal includes both. Publicly available specifications means specifications produced by industrial communities (e.g. Open group, PKCS specifications), which may not have formal recognition as standardization bodies, but are open to unrestricted public use and have become widely adopted as a de-facto standard.

The consultation procedure is as follows:

1. The representative of the Commission submits to the Committee a draft of the measures to be taken.
2. The Committee delivers its opinion on the draft within a time-limit which the Chairman may lay down according to the urgency of the matter.

The Commission adopts measures that shall apply immediately. However, if these measures are not in accordance with the opinion of the Committee, they shall be communicated by the Commission to the Council forthwith and the application of the measure shall be suspended for three months. The Council may then take a different decision within this time limit.

EESSI Recommendation*: The "Electronic Signature Committee", which is composed of representatives of the Member States and the Commission would need to get advice from the industry. To this respect, EESSI recommends the establishment of an “Electronic Signature Industry Advisory Group” to provide advice and recommendations to the "Electronic Signature Committee". The "Electronic Signature Industry Advisory Group" should be composed of recognized technical experts in the area of electronic signatures from the vendor and user industry*

3.10 Information, Implementation and Reviewing rules

Member States are obliged to inform the European Commission on the following:

- voluntary national accreditation regimes, including any additional requirements pursuant to Article 3.7;
- names and addresses of the national bodies responsible for accreditation and supervision; as well as the bodies referred to in Article 3.4 ;
- the names and addresses of all accredited national CSPs.

Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive within 18 months after entry into force of the Directive. Taking into account the European Parliament elections in June 1999 delaying the adoption procedure of the Directive, it may, however, be expected that the Member States will have a harmonized common framework on electronic signatures before the end of the year 2002.

The Commission will bring forward a review of this Directive two years after its implementation in part to ensure that the advance of technology or changes to the legal environment have not created barriers to achieving the aims stated in this Directive.

4. A Framework for Electronic Signature Standardization

4.1 Objectives for EESSI

From the Directive, the HLSG report on Electronic Signature and other relevant input documents, two priority areas of standardization can be identified:

- standards by which a CSP may be assessed and/or certified as to meeting the security and functional requirements of the Electronic Signature Directive
- standards for products which can be used by signers and verifiers to be assured that electronic signatures are secure and have legal effect under the Directive (or national laws implementing the Directive)

There is also a strong requirement for technical interoperability standards for electronic signature functions, in order to achieve interoperability between products and services:

1. Users want standardized and interoperable products to enable them to buy different components from different vendors.
2. Vendors want standards to enable them to sell products on an international market.

As a means for providing an open competitive marketplace for implementations of electronic signature services and products, the following interoperability standards are therefore required:

- between signers and verifiers (e.g. syntax and encoding of electronic signatures)
- between signer and CSP
- between verifier and CSP
- between signer / verifier and local signature device (e.g. smart card),
- between CSPs.

It is the objective of the Directive to be non-discriminatory and implementable with as wide as possible range of technologies. However, it is also recognized that it is very difficult to define a common basis against which implementations may be judged without selecting a particular technology for electronic signatures.

For this reason, EESSI has also identified the need for selecting a first set of presently recognized technologies and mechanisms to be used for electronic signatures. This is further described in section 4.3. However, wherever possible generic frameworks for procedures and practices are recommended.

4.2 Classes of Electronic Signatures for standardization

The qualified electronic signature

Article 5.1: Member States shall ensure that *advanced* electronic *signatures*, which are based on a *qualified certificate* and which are created by a *secure creation device* satisfy the legal requirement of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies that requirement in relation to paper-based data, and are admissible as evidence in legal proceedings.

In order to be able to make reference to electronic signatures fulfilling all the requirements of article 5.1, we have in this report introduced the following definition:

> A **qualified** electronic signature is a signature that fulfils all the requirements of Article 5.1

By fulfilling these requirements, legal acceptance is recognized for advanced electronic signatures fulfilling these minimum technical security requirements. There is then obviously a need to standardize these requirements to enable conformity assessment, but also to achieve a harmonized (e.g. agreed minimum) level of security across Europe.

The need for general requirements for electronic signatures

One important question is: Do we also need to standardize any aspect of technical security for legal value according to article 5.2?

When using electronic signatures, users are primarily concerned with achieving well-defined and acceptable quality of security and liability. One method of achieving a degree of assurance of the security is through the management of the supporting services. By applying standards to the management of security, such as managing the risks, auditing operation, identifying personnel with specific responsibilities for security, it is possible to achieve a degree of harmonization. Whilst this may not be given the same degree of assurance in the level of protection as the placing specific requirements on the provision of supporting service (as in annex II), there are definite advantages where technology independence is a concern. This approach is of particular relevance to the requirements of general electronic signatures given in 5.2 of the Directive.

The need for enhancements to the electronic signature

Another important question is: Do we only need to standardize the minimal technical security requirements for electronic signatures resulting from the Directive, or do we have to go further to enhance the technical security? From a legal point of view, the signer does not need to fulfil other requirements than those mentioned in article 5.1. However, it should be made clear that only a minimum level of technical security is reached when solely fulfilling the article 5.1 requirements. Thus, on their own, the requirements placed on the signer for the production of qualified electronic signatures may not be sufficient for a verifier or an adjudicator as technical evidence to settle some disputes.

For example, consider the case when an electronic signature is supported by a certificate which has been revoked some time after the signature was created. In order to settle a dispute over such an electronic signature, it is necessary to provide evidence that shows that the certificate was still valid at the time the signature was generated. Thus, independent evidence of the time that the signature was created is required to prove that certificate was not revoked at the time the signature was generated. This can be achieved through a Time Stamping Authority (TSA) which binds a time-stamp to signed data. Hence, many consider that a TSA is an important component of electronic signature infrastructure.

Time-stamping and other enhancements can in certain cases thus be required for both general and qualified electronic signatures. In this report, we have therefore also considered standardized enhancements to the baseline requirements for general and qualified electronic signatures to address commonly recognized threats. We call these “enhanced electronic signatures”.

Different types of electronic signatures

In summary, there is a need for standardization for various types of electronic signatures, as described in the following table.

Type of signature:	**General electronic signature** as required in 5.2	**Qualified electronic signature -** as specified in 5.1 (Annex I, II, III)	**Enhanced electronic signature** (applicable to both general and qualified electronic signatures)
Level of legal certainty:	Can not be denied legal effect (art 5.2)	Same legal effect as hand-written signature (art 5.1)	Enhancement of technical evidence
Explanation:	Any electronic signature that is not a qualified electronic signature.	Minimum technical level required for the signer so that his electronic signature can be considered as legally equivalent with a hand-written signature.	Additional technical requirements for a verifier, such as time-stamping, but also for the signer, to enhance technical security and obtain protection against certain threats.

The EESSI work will primarily focus on the middle column, i.e. standardization for qualified electronic signatures. However, in some places, the report will indicate general requirements for electronic signatures as well as additional requirements for enhanced electronic signatures.

4.3 Technical framework for qualified electronic signatures

The Directive is not strictly technology neutral; for qualified electronic signatures, it mandates the use of a specific set of mechanisms, namely certificate-based asymmetric cryptography using Certification Authorities. The Directive, and in particular annexes I and II, identifies requirements for Qualified Certificates and CSPs creating such certificates. The Directive thus implicitly defines a "technical framework".

For this framework to be fulfilled in a consistent manner, providing a common level of quality and functionality, it is considered necessary to define one or more agreed sets of components (security mechanisms and technologies). Thus the approach should be to specify one or more "sets of components" that can be used to fulfil the technical framework which supports qualified electronic signatures. Then, any specific management requirements for supporting those components (e.g. certificate policy) shall be identified. Also, specific security requirements and practice statement requirements relating to the set of components shall be identified. Finally, technical profiles need to be established on how the technical standards for CSP (e.g. certificate formats, certificate management protocols) should be employed to meet the technical framework requirements.

In Annex III, the Directive also identifies requirements for the protection of the private key. Several types of hardware devices are able to meet the requirements of Annex III, such as smart cards, PCMCIA cards and Personal Digital Assistants (PDAs). Standardization for using these devices for electronic signatures is needed. However, nothing precludes, and we also foresee, that other devices will rapidly be standardized to fulfil the requirements of annex III.

EESSI Requirement*: Specification of one or more sets of components fulfilling the technical framework for Qualified Electronic Signatures.*

EESSI Initial Recommendation:

The following set of components mechanisms, described in standards and publicly available specifications, are proposed as a first set of components that can be used for qualified electronic signatures:

- *Authentication framework using X.509 certificates [ISO/IEC 9594-8]*
- *X.509 PKI Certificate and CRL Profile [RFC 2459]*

- *Digital signatures using the RSA and DSA algorithms [ISO/IEC 14888-1, -3]*
- *Hash functions SHA-1 and RIPEMD-160 [ISO/IEC 10118-3]*
- *Cryptographic Message Syntax [RFC 2315] based on RSA's publicly available specification PKCS #7*
- *Use of hardware tokens, such as smart cards [ISO/IEC 7816 part 4-9, DIN Vornorm 6629 and/or RSA's specification PKCS#15], PCMCIA cards and Personal Digital Assistants (PDAs) for secure storage and usage of private keys.*

The reasons for choosing this particular set of technologies are the following:

- These technologies are generally accepted and already widely deployed in a number of countries
- Standards exist for the use of these technologies.
- There is an urgent need for a set of technologies which can used to provide a complete standards based solution.

It should be noted that there exists another cryptographic technique based on the use of asymmetric cryptography, namely identity-based digital signatures that can be used for electronic signatures. However, this technology is not yet widely deployed.

Elliptic Curve Cryptography presently looks very promising and standards exist for this technology. As soon as it starts to get more widely deployed, it will most likely be included in the set of components.

4.4 A layered framework for regulation and standardization

Introduction of a framework for electronic signatures requires a combination of legislation and technical standards. At one end, we will have the Directive and national legislation introduced to support electronic signatures according to the Directive. At the other end, we have technology and a number of technical standards that presently can be used for electronic signatures, for example digital signatures, hashing algorithms, certificates, cryptographic algorithms etc.

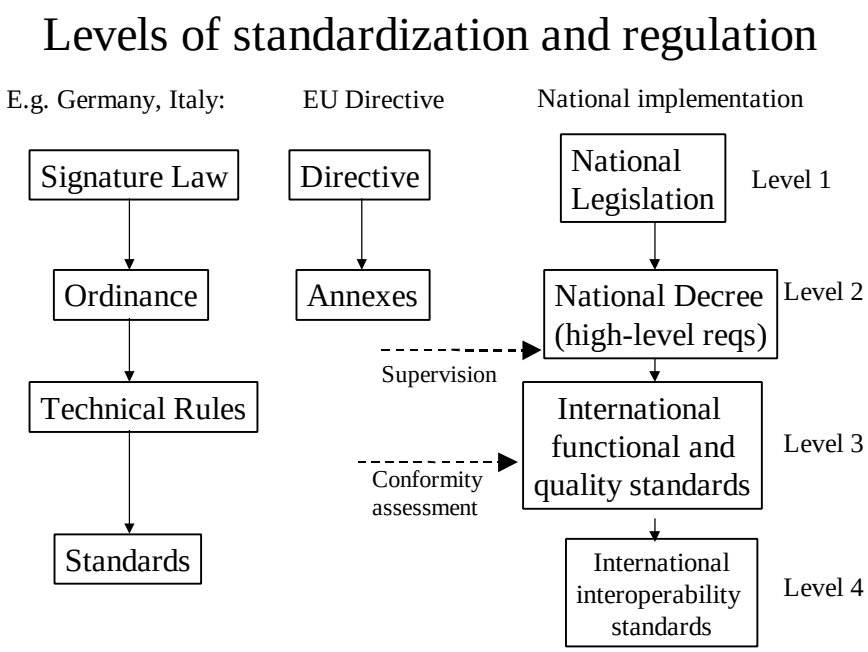
What we need to define is a »layered standardization framework» that binds these two ends together in an appropriate way. In both Germany and Italy for example, this has been achieved through a layered legal structure:

- Signature Act
- Signature Ordinance
- Technical Rules
- Existing standards

If the same effect is to be achieved to support the Directive, there is a need for a division of responsibilities between legislation and standardization. We also need a harmonized way for specifying how legislation can refer to standards.

A general observation by independent experts is that Germany and Italy have made too much use of the legislative instrument to detail the technical requirements, instead of standardization. The German Signature Ordinance and the Italian Technical Rules could equally well have been implemented as national standards.

The EESSI recommendation is to minimize the legislation and keep it very general. Technical standards developed and supported by the industry can then supply the basic necessary framework, as described below.



Level 1: Legislation

- Technology independent.
- Contains general legal requirements corresponding to the main body of the Directive (e.g. equivalence to written signatures, optional accreditation etc.)
- Outside the scope of EESSI

Level 2: High level requirements

- Extensible range of technologies supporting electronic signatures
- Defines basic functional requirements in accordance with the Annexes of the Directive
- Points out a national regulatory body that is empowered to prescribe standards in this area, i.e. standards at level 2 below.
- This level is most likely implemented as a decree or regulation
- Outside the scope of EESSI

Level 3: Functional and quality standards

- Dependent on technology and style of operation of its use to support electronic signatures
- For a given set of technologies, the standards define detailed requirements fulfilling the high level requirements, for example:
  - Standards for secure management and operation of a CSP
  - Security standards for signature products
- A scheme for voluntary accreditation/certification of CSPs and conformity assessment of signature products.

At this level, we have to find a solution to the following dilemma: "How can security standards for electronic signatures achieve a common and well-defined level of security whilst at the same time cater for the "rapid development of technology and the global character of the Internet [which] necessitate an approach which is open to the range of existing and potential future technologies and services …."?

The approach taken in the Directive, and also by the EESSI, is that it is not possible (or more correctly: not economically feasible) to specify and build an absolutely secure system, resistant to all possible threats. Instead, a balance has to be found between the costs involved and acceptable business risks.

Level 4: Technical interoperability standards

- Define specific use of technology to support electronic signatures
- Facilitate interoperability between
  - Signer <-> verifier
  - Signer/verifier <-> local device
  - Signer/verifier <-> CSPs
  - CSP <-> CSP

This is definitively needed by the industry.

4.5 Areas requiring standards and conformity assessment

The Directive describes several areas that may require standardization and conformity assessment of product and services to those standards:

- Voluntary certification of CSPs (Art 3.1)
- Supervision of CSPs (Art 3.3)
- Standards for trustworthy systems and secure signature creation devices (Art 3.5)

In addition, there may be a need for additional standards and voluntary conformity assessment also in the following areas:

- Signature verification products (Only recommendations in Annex IV)
- Secure signature creation environment (Excluded in preamble 15)

Article 3.4 of the Directive also requires that the conformity of secure signature creation devices against the requirements of Annex III be "determined" by appropriate bodies. The criteria for "designating" such bodies is to be established "pursuant to the procedures laid down in Article 9". This assessment of conformance against annex III of the directive has similar implications to conformance assessment of devices against standards recognized under Article 3.5. Thus it is considered that these processes need to be aligned.

***EESSI Recommendation**: Conformance assessment of secure signature creation devices against Annex III under Article 3.4, and the scheme for conformance assessment of standards for electronic signature products that may be recognised under Article 3.5 should be aligned.*

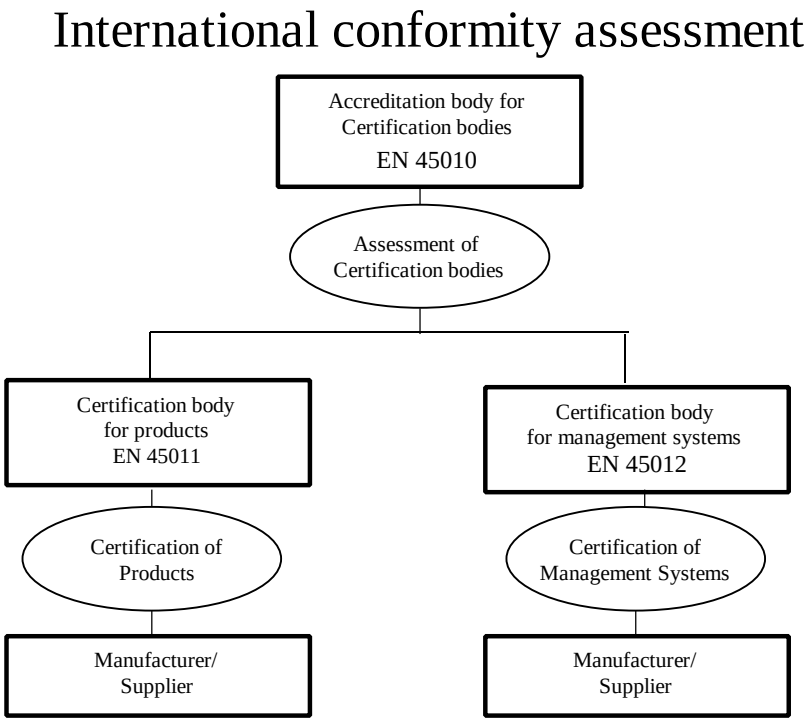
Chapters 5 and 6 describe the requirements of standards against which conformity assessment can be performed, for CSPs and for products. All these standards can be said to belong to Level 3 of the framework model (Functional and quality standards). There is also a need for technical interoperability standards (Level 4). These are described in chapter 7.

It is currently somewhat unclear to what extent the Directive prescribes mandatory conformity assessment. The remaining part of this chapter discusses various aspects of conformity assessment.

4.6 Accreditation and certification

The standards EN 45010, EN 45011 and EN 45012 specify accreditation of certification bodies for products and management systems. The standards are also published by ISO/IEC as Guides 61, 66 and 62. In Europe, each Member State has a nationally recognized Accreditation Body,

which performs such accreditation (e.g. SWEDAC, COFRAC, UKAS, RvA). Detailed guidance for information security management systems is being defined in EA-7/0X. This is illustrated in the following diagram.



The accredited Certification Body performs assessment and certification of organizations according to a specific functional, management, quality or technical standard. The European co-operation for Accreditation (EA) ensures mutual recognition within EU/EFTA for mutual recognition of certifications. For more information on EA, see Annex A.1.8.

From the viewpoint of Electronic Signatures, assessment may be required for the qualitative, management and function aspects of both the signature creation / verification products and CSPs used to support electronic signatures. Standards are then necessary against which such assessment can be made. These standards will of necessity relate to a set of selected technical solutions, since different styles of operation will have widely differing functional requirements. However, they do not need to go into the details of the specific use of technology necessary to meet the requirements of interoperability. Hence the decision has been made in this report to clearly delineate the level 3 functional / qualitative standardization requirements needed for assessment of a product or service, and the level 4 standardization requirements relating to interoperability.

For the signature products requiring conformity assessment according to the directive (secure signature creation devices and trustworthy systems), there are presently no general standard criteria for accreditation of certification bodies. Such criteria are currently tied to the specific security evaluation scheme (e.g. ITSEC, Common Criteria etc).

Consideration also needs to be given to requirements for accreditation schemes which are globally recognised to enable cross recognition of products and services certified outside Europe. In addition, industry lead schemes such as those being developed under the Emeritus project should be considered.

EESSI Requirement: *Standard criteria for accreditation of certification bodies performing conformity assessment of signature products, as well as guidelines for performing such assessment.*

EESSI Recommendation: *Where conformity assessment is to be determined by a certification body designated by a Member State (e.g. as required under Article 4 of the Directive) through a*

national authority, it is recommended that they are selected under the equivalent criteria as for certification bodies accredited under the European accreditation scheme operating under EN 45010. Consideration also needs to be given to requirements for globally recognition of accreditation schemes and Industry lead certification / accreditation schemes.

4.7 The New Approach and European Conformity Assessment

The New Approach

In 1985, the Commission introduced a new strategy to complete the internal market for goods in a White Paper. The strategy is called The New Approach. It is further elaborated in the Council´s Resolution on a new approach to technical harmonization and standards.

New approach directives shall contain the essential requirements to be fulfilled to provide for protection of life, health environment etc. These requirements must be fulfilled before the product can be lawfully placed on the market. It is left to standardization bodies to draft standards that contain detailed technical specifications on how to fulfil the essential requirements. Use of these standards (harmonized standards) remain voluntary, but give presumption of conformity to the essential requirements. New approach directives also contain conformity assessment procedures, making provisions, safeguard clauses and free movement clauses. The directives are normally totally harmonizing, i.e. Member States must see to that all provisions of the directive are met before the product is placed on the market and at the same time Member States must ensure free movement for goods complying with the directive. A Manufacturer's Declaration should, according to the new approach, normally be sufficient. If a manufacturer uses other technical specifications than harmonized standards instead, third-party involvement is envisaged.

For more information on the New Approach, see: http://www.newapproach.org/

Manufacturer's Declaration

The most simple form of a Manufacturer's Declaration is a statement made by the manufacturer that a product/service is produced in a way that ensures compliance with the requirements set out in regulations, acts, technical standards or other normative documents. Such declarations are typically made in accordance with ISO/IEC Guide 22 (EN 45014).

The Manufacturer's Declaration can thus be a direct alternative to traditional third-party certification or testing. In this case, the declaration is often combined with a requirement on the manufacturer to demonstrate how he has ensured that the product/service complies with the stipulated requirements. One way of doing this is to use an accredited laboratory. Additionally or alternatively, the manufacturer can be required to have an appropriate quality system in place in order to be allowed to make the Manufacturer's Declaration.

Conformity assessment in the European Community

The New Approach was completed with a Council Decision concerning a system for conformity assessment, i.e. assessment that a product is in conformity with the essential requirements in the relevant directive. The Global Approach contains a number of "modules" that may be used to show conformity. The modules entail both the design and the construction phase of the product. They can be more or less burdensome for the manufacturer; from manufacturer's declaration of conformity through type approval to unit verification and full quality assurance. In a new approach directive, the choice of what modules should be used is made in the directive. This choice is based, among other things, on the risks of the products concerned.

The aim of this system is to achieve mutual recognition of testing and conformity assessment in the EU, both in the mandatory and voluntary area. The criteria for the bodies concerned must be clear, uniform and objective so that Member States and others relying in the results have confidence in the system. Such criteria for testing laboratories and for certification bodies are contained in the harmonized European Norms, EN 45000. These standards also contain norms for conformity assessment of the certification bodies as well as requirements on the accreditation bodies. The EN

29000 standard contains requirements for quality systems. All third party conformity assessment is performed by so called notified bodies. Usually, these are accredited certification bodies. The EC Member States shall notify to the Commission the bodies that are accredited for conformity assessment. The Member State is responsible for that the notified body conforms to the requirements of the relevant directive.

Self Regulation by Industry

A further alternative approach which may be used for assessment of certification service providers is through self-regulation. An example of this is being developed under the Emeritus project which envisages a model based on a Global Trust Services Federation (GTSF) made up of a Trust Services Association (TSA) in each nation. The activities of the Federation is to include, where this is allowed by national laws, the accreditation of service providers against criteria which give subscribers some assurance of the quality of service offered by individual TSPs.

This approach provides a mid way between the EN 45000 based accreditation scheme which is rigidly controlled from the top down, and the liberal Manufacturers Declaration.

Conformity assessment for the Directive on Electronic Signatures

The electronic signatures Directive is not a new approach Directive in the strict sense. It is the first occurrence of a new kind of Directive based on the "light and flexible regulatory approach of high-tech issues". Due to the nature and characteristics of emerging new technologies, only the strict minimum necessary to ensure the most important factors is covered by such a Directive. Compliance with Annex III, or the standard implementing Annex III of which the number has been published, is regarded to be such a factor, and can only be determined by a notified body.

However, it is the opinion of EESSI and the industry that Manufacturer's Declarations also should be allowed and valid. Conformity assessment of CSPs and signature products should be possible in three different ways:

a) Formal assessment and certification by an accredited certification body. Such external assessment is normally performed before the start of operation or sale (a priori).

b) Manufacturer's Declaration, which specifies that the manufacturer conforms to the required standards, and has applied an appropriate quality control procedure. Verification of such a claim may either be performed a priori, as above, or later, for example after a dispute (a posteriori). Manufacturer's Declaration does not exclude testing, certification and inspection by an external laboratory. It is just an alternative way of demonstrating that quality assurance of a product or service is performed in an acceptable manner.

c) Self regulation with assessment carried out by an industry led federation of service providers.

4.8 Supervision of CSPs

Article 3:3: Each Member State shall ensure the establishment of an appropriate system which allows the supervision of Certification Service Providers established on its territory which issue qualified certificates to the public.

The concept of supervision in this article, and its relation to the «voluntary accreditation scheme» in Article 3.1 is somewhat unclear. It can be interpreted as follows:

- An appropriate government or private body shall be appointed for supervision of CSPs issuing qualified certificates.
- Supervision does not mean licensing or prior authorization. Instead, it is a procedure to continuously monitor and ensure that the CSPs fulfil the general requirements laid out in the Annex II (or rather: as they have been re-formulated in the national «Level 2» decree/regulation), and that their certificates conform to Annex I.

- Most requirements in Annex II are also further detailed in standards at «Level 3» and thus assessed in the voluntary certification, for example (i): «not store or copy signature creation data…».
- Some requirements in Annex II are ONLY assessed in the supervision process, for example (g): «maintain sufficient financial resources…».

It should be pointed out that there is no implicit relation between such a «supervised CSP» and a «certified CSP». A CSP may be supervised (issuing qualified certificates according to Annex I and II), certified (fulfilling a specific set of standards, but not issuing qualified certificates, and thus not supervised) or both.

4.9 Signature policies and certificate policies

Electronic signatures are commonly applied within the context of a legal or contractual framework. This establishes the requirements on the electronic signatures and any special semantics (e.g. agreement, intent). These requirements may be defined in very general abstract terms or in terms of detailed rules. The specific semantics associated with an electronic signature implied by a legal or contractual framework are outside the scope of this study.

However, of general concern for electronic signatures are the specific requirements for the creation and verification of electronic signatures independent of the specific semantics. These rules have to be recognized as meeting the requirements of the legal / contractual framework (for example, by direct reference, through accreditation or by accepted reasoning). These rules and requirements may include, for example:

- Rules for signature creation, including use of specific electronic signature devices, syntax and signature algorithms.
- Rules on the use of CSPs (supporting certification and other functions such as time-stamping).
- Rules for signature verification including the need to maintain time-stamped records of validation data.

Another important fact that needs to be agreed between signer and verifier is the type of commitment made by the signer by applying his signature.

Without agreement on such detailed rules, the signer and verifier are uncertain as to what may be recognized by the other party as a valid signature. This set of rules is referred to, in this document, as a **signature policy**. A signature policy may be implied by the collection of rules that are applied by the signer and verifier, or formalised in a single specification that can be referenced (named).

In this document, a **signature policy** is defined as:

> "a named set of rules for the creation and verification of an electronic signature, including any use of CSPs, that is recognized as being valid within a given legal / contractual context."

A signature policy may be defined, 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. The standards identified in this document may be used as the basis for a signature policy meeting the requirements of the Directive.

Certificates, supporting electronic signatures, are commonly issued under a **Certificate Policy**. This is defined in X.509 as

> "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."

A certificate policy generally includes undertakings by:

a) the certificate issuer (CA) (e.g. verification of subjects when registering, maintenance of audit logs, delays and means for the notification of revocation) as well as

b) obligations of signers (e.g. maintaining secrecy of the private key) and

c) requirements on relying parties in the proper use of certificates in validating signatures.

Many of the signature policy requirements on signers will be met by the rules in a certificate policy. Hence, many of rules of the signature policy for the signer side may be established just by reference to the acceptable Certificate Policies. However, some aspects of signature policies are outside the scope of the certificate policies (e.g. the use of time-stamping services, archiving) and hence need to be established independent of the Certificate Policy.

Whether or not a certificate policy is used by the CSP, the signature policy needs to establish rules for the use of CSPs. In the simplest case, this can be a list of trusted CSPs but it can also include the certificate policies that are acceptable as well as constraints on the CSPs such as naming and key usage.

Standardization requirements for Certificate Policies are identified in chapter 5; the standardization implications of Signature Policies have yet to be established.

EESSI Requirement*: Study of the standardization implications of Signature Policies.*

5. Functional and Quality Standardization for CSPs

This chapter describes the requirements for functional and quality standards for CSPs (Level 3 of the standardization framework model), as well as the corresponding conformity assessment.

Certification Service Provider, as defined in the Directive, encompasses all types of trusted service providers related to electronic signatures.

This includes services relevant to CSPs issuing qualified certificates:

- Certification authority services
- Registration authority services
- Directory services

It also includes additional services which may be used to support electronic signatures, such as:

- Time-stamping services
- Attribute Authority services
- Trusted archival services
- Notarisation services

This chapter considers:

a) General standardization requirements that are applicable to any of the above CSPs, whether or not they support qualified electronic signatures.

b) Standardization requirements for CSPs issuing qualified certificates (Certification Authorities with associated registration and directory services).

c) Standardization requirements for additional services which can be used to support electronic signatures.

For each of these areas this chapter discusses requirements for:

- The management of the CSP security to ensure that the appropriate quality is assured;
- Use of trustworthy systems for running the CSP services as necessary to achieve the required assurance in the implementation;
- Technical profiles which provide the functionality necessary to meet the service requirements (detailed technical and interoperability requirements are discussed in section 7);
- Policy and practice statements providing a coherent framework for the overall security of operation of CSPs including all the relevant technical and management aspects;
- Conformity assessment.

This report considers the services relevant to CSP issuing qualified certificates (certification authority, registration authority, directory) as a whole. Whilst these services may be provided independently it is considered that in the short term one body should be given overall responsibility for the provision of these services to the user. Thus, currently requirements for qualitative standards for CSPs issuing qualified certificates are considered as a whole. However, it may be necessary to within these standards to clearly delineate the responsibilities between providers of the different services.

5.1 General CSP Requirements

5.1.1 CSP Security Management

To achieve some assurance of the secure operation of a CSP for general electronic signatures, as well as for qualified electronic signatures, there is a need to establish codes of practices for the secure management of the CSP, independent of the services provided.

There are "codes of practice" standards for the management of information security, which are commonly accepted. They include practices for the identification of security risks as well as the application of the appropriate controls to manage those risks. Three such standards and publicly available specifications are:

- BS 7799 Part 1 (1999): Code of Practice for Information Security Management (BS7799 is described in more detail in Annex A.5; also a detailed comparison between BS 7799 and Directive requirements is given in Annex C.1)
- ISO TR 13335: Guidelines for the Management of Information Technology Security-GMITS
- COBIT (Control Objectives for Information and Related Technologies) specification produced by the Information Systems Audit and Control Foundation.

BS 7799 Part 1 has been already used in a number of countries in Europe and around the world, and is likely to be proposed for standardization internationally.

Such codes of practice place little or no constraint on the services that can be offered by the CSP and give the signer and verifier a degree of assurance that the electronic signature is not weakened by poor security management of the CSP.

***EESSI Requirement**: European recognition of standard security management guidelines (e.g. BS 7799, ISO TR 13335, COBIT) generally applicable to CSPs supporting electronic signatures.*

For the voluntary certification of CSPs against a code of practice, specific requirements need to be identified. The ISO TR 13335 gives a large amount of guidance that should be followed as considered appropriate. The application of the guidelines is left up to the service provider. For the security management of the CSP to be certified then specific requirements need to be identified against which a CSP may be certified. BS 7799 (1999) includes a second part which details the use of risk analysis as a basis for management procedures and controls against which a service provider can be certified.

Such a specification may be used for formal certification using an accredited body, or for the issuance of a Manufacturer's Declaration.

Currently, there are no plans to standardize BS 7799 part 2 internationally.

***EESSI Requirement**: European recognition of Specific Requirements for Assessment of Security Management (e.g. as in BS 7799 part 2) generally applicable to CSPs supporting electronic signatures*

5.1.2 Use of Trustworthy systems

Whilst this requirement is identified in the Directive only in relation to CSPs issuing qualified certificates, the same general requirements for use of trustworthy systems may be applied to all CSPs in supporting other services such as time-stamping and notarization. The only difference is that use of such systems is only required when issuing qualified certificates.

The CSP security management discussed in the previous section is the most important factor the creating trust for a CSP. However, there is also a need for a CSP to show that it uses trustworthy systems and products in its operation. To a certain extent, this can be achieved by the risk assessment and accompanying preventive measures, but there may also be a need for providing standards specifying minimum requirements for such "trustworthy systems and products".

The selection of the appropriate assurance level for implementations may be left open, to be done on a case by case basis, if the use of risk analysis, and other security management practices (see 5.1.1), can assure that appropriate selections are made. However, where risks are generally recognized as being high and requiring special countermeasures, such as with the handling of cryptographic modules, standardization is more important.

***EESSI Requirement**: General requirements for use of trustworthy systems and products by CSPs*

***EESSI Initial Recommendation:** CSPs should use trustworthy computing platforms as required by their risk analysis under security management standardization*

5.1.3 Technical Profile Requirements

Requirements for technical standards will depend on the services being supported.

5.1.4 Policy and practice statements

If CSPs are to be given the freedom to decide how they are to operate, the services to be provided, the mechanisms used and the signature protocols to be supported, it is important that there is transparency. If signers and verifiers are to properly assess whether the CSP is fit for their purposes they need to have available sufficient details of the CSP operation to make that assessment. Thus, standards are considered necessary which specify the information that CSPs should provide on the practices, and how this should be made available to subscribers. Ideally this information would be made publicly available, however, commercial reasons may limit its availability.

BS 7799 includes requirements for the production of security policy documentation. This documentation may be also be used by CSP subscribers as a basis of assessing the operations of the CSP.

A registration scheme for contractual terms and conditions is being established by ICC (called E-terms). Use of such a registration scheme can provide an independent source of a CPS which is unambiguous and independent of the service provider.

***EESSI Requirement**: Standard for the documentation of CSP Policies / Practice Statements.*

5.1.5 Conformity Assessment

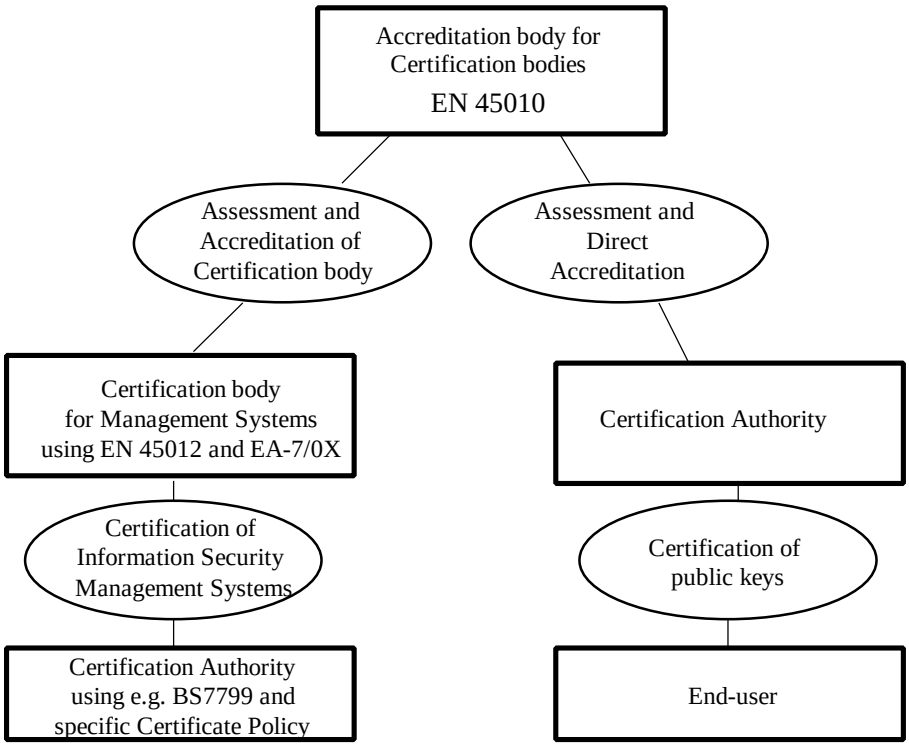
Article 3.1: Member States shall not make the provision of certification services subject to prior authorization.

Article 3.2: Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification service providers for reasons which fall under the scope of this Directive.

It should be pointed out that accreditation/certification is not required for the possible legal effect or not of an electronic signature. However, a signature created with a certificate from an accredited/certified CSP may have stronger evidence value in court. Certification is therefore most likely achieved by a CSP in order to increase the market confidence in its services.

The general conformance requirement of a CSP supporting electronic signatures, placing minimal restrictions on the technology, is conformance to security management codes of practice as described in 5.1.1. This should be supplemented by requirements on the documentation of CSPs practices as described in 5.1.4.

It should be pointed out that there are currently two possible models being discussed in Europe for accreditation/certification of CSPs, as described by the figure above:



- Assessment and certification by certification body under accreditation. This is the normal procedure for certification of organizations.
- Direct accreditation by an accreditation body. The CA is then regarded as a "certification body", since it issues certificates containing "certified information". The difficulty with this scheme is that there exists no standard today for accreditation of such bodies (i.e. CAs). Also, there exists no standard today against which such bodies can be assessed. BS7799 would not be sufficient in this respect.

Mutual recognition of accreditation/certification in this area is assured through EA and its "Guideline for the Accreditation of bodies operating certification/registration of Information Security Management Systems" (EA-7/0X).

A third possibility is through self-regulation by an industry led federation of CSPs such as being established through the Emeritus project.

It is required that the names and addresses of certified national CSPs are reported to the Commission and other Member States (article 11:1c).

In summary, conformity assessment of all types of CSPs supporting electronic signatures is generally required against General Security Management requirements for CSP (see 5.1.1)

EESSI Requirement*: General conformance assessment scheme for CSPs.*

EESSI Initial Recommendation: *A Conformance Assessment scheme needs initially to be set up using EN 45012, BS7799 and EA-7/0X with self-regulation as a potential alternative.*

5.2 CSPs Issuing Qualified Certificates

5.2.1 CSP Security Management

The following Annex II requirements would be addressed by a general standard for CSP Management as identified in 5.1.1:

Annex II: Certification service providers must:

(a) demonstrate the reliability necessary for offering certification services;

(e) employ personnel which possesses the expert knowledge, experience, and qualifications necessary for the offered services, in particular competence at the managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also exercise administrative and management procedures and processes that are adequate and which correspond to recognized standards;

The following requirements of Annex II are considered specific to qualified electronic signatures, and need to be addressed by enhancements to the general requirements for management and operation of CSPs in 5.1.1:

Annex II: Certification service providers must:

(b) ensure the operation of a prompt and secure directory and secure and immediate revocation service;

(c) ensure that the date and time, when a certificate is issued or revoked, can be determined;

(d) verify by appropriate means in accordance with national law the identity and if applicable any specific attributes of the person to which a qualified certificate is issued;

(g) take measures against forgery of certificates, and, in cases where the certification service provider generates signature creation data, guarantee the confidentiality during the process of generating that data;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular to provide evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature creation data of the person to whom the certification service provider offered key management services;

A general security management approach using risk analysis may lead to the appropriate controls being put in place. However, as identified in Annex C to this report, general codes of practice for information security management such as BS 7799 do not provide any detailed guidance as to how certification service providers can meet the specific requirements of Annex II to the Directive.

In order to establish a common means of meeting the Annex II requirements on CSPs issuing qualified certificates, it is considered necessary to extend and refine the general information security management controls to address all the requirements of such a CSP. It is suggested that such a standard should build on the standardization identified in 5.1.1.

A draft technical report being developed by ISO/IEC (PDTR 14516) provides guidance on the use and management of TTP (Trusted Third Party, equivalent to a CSP in the terminology used by this document). This, however, is not targeted at the specific requirements of Qualified Electronic Signatures and does not identify any specific requirements against which a CSP can be certified.

Other sources of potential requirements, which may need to be studied to identify the particular requirements of advanced electronic signature, include:

a) The German BSI Safeguard Manual for Digital Signatures,

b) The American Bar Association PKI Assessment Guidelines (formerly called PKI Evaluation Guidelines)

c) The Australian Government PKI Criteria for Accreditation of Certification Authorities

d) The Government of Canada PKI certificate policies

***EESSI Requirement**: Security Management requirements for CSPs issuing Qualified Certificates*

***EESSI Initial Recommendation**: This may partially be met by a BS 7799 equivalent but would be more effective if requirements for CSP specific controls were addressed.*

The requirements on CSPs currently given in annex II of the Directive do not clearly delineate the obligations relating to the separate services that are necessary for a CSP issuing qualified certificates. Such a CSP can involve a certification authority, registration authority and a directory service provider, each of which may be separately managed. In such a situation the responsibilities of each of the separate service providers needs to be clearly identified. This is an area which requires further study.

EESSI Requirement: *Study of the separate responsibilities of a certification authority, registration authority and directory service provider in supporting Qualified Certificates.*

5.2.2 Use of Trustworthy systems

> Annex II: Certification service providers must:
>
> (f) use trustworthy systems and products which are protected against modification and which must ensure the technical and cryptographic security of the processes supported by them;

The general considerations for use of trustworthy systems given in 5.1.2 are also applicable to CSPs supporting qualified certificates.

However, for CSPs issuing qualified certificates, a specific requirement regarding the use of trustworthy systems can be found in Annex II. According to the Directive (Art 3.3), references to standards for such products will be published by the Commission.

Presently, the German and Italian regulation for digital signatures has set such requirements, based on the ITSEC assurance levels. In Germany, the BSI Manual for Digital Signatures provides additional guidelines. In United States, several states are requiring CSPs to conform to the CS-2 Protection Profile, based on Common Criteria. The CS-2 Profile, although focusing on a "security target", also to some extent covers security management. The Open Group has also published the "X/Open Baseline Security Services (XBSS)" and "Baseline Security 96", which can be used for self-assessment by product suppliers.

The Common Criteria may be considered to have advantages over the ITSEC criteria as it represents the latest thinking on how criteria should be established and is being standardized on a global basis. For further details of the alternative criteria and associated protection profiles see Annex A.5.

The American FIPS140-1 standard specifies security requirements for cryptographic modules and is thus more specific to the protection of private keys and support of cryptographic functions in a trustworthy system, and can be suitable for that purpose.

***EESSI Requirement**: Security requirements for trustworthy systems and products used by CSPs issuing Qualified Certificates*

EESSI Initial Recommendation:

- *Security requirements for cryptographic modules should be specified using FIPS 140-1 or a European equivalent.*
- *A Common Criteria Protection Profile for CSPs should be developed, possibly based on the CS-2 profile.*

5.2.3 Technical Profile Requirements

Whilst details of technical interoperability are more appropriate to Section 7, when establishing qualitative and functional standards it will be necessary to select specific technical profiles to detail

the particular functionality required. No separate standards exist which specify the functional (service) requirements independent of the technical solutions. Thus it is proposed that specific functional requirements have to be specified in terms of selecting specific technical standards.

Technical standards generally exist for all the component services and mechanisms required for qualified electronic signatures. However, because there are many variations of these standardized protocols and data formats, there is a need to specify a profile for the use of these standards.

To get a consistent level of quality in the strength of such certificates, technical profiles should also include recommendations on the algorithm and key lengths used in signing certificates.

The technical standards can be separated into two aspects: those that support the operational use of certificates and those that support the management of certificates. It is considered that the first is of most concern to the open standards environment. The management of certificates is only of concern to those users who directly subscribe to a CSP for their own certificates. Whereas, the operational aspects are of interest to all those using those certificates for signature verification.

***EESSI Requirement**: Technical Profile for operational aspects of CSPs issuing qualified certificates.*

***EESSI Initial Recommendation:** It is recommended that this profile consists of:*

a) Profile for use of X.509 Public Key Certificates to meet the requirements of Annex I of the Directive.

The suggested basis for this profile is the following two documents from the IETF PKIX working group:

- *Internet X.509 PKI Certificate and CRL profile (RFC 2549)*
- *Internet X.509 PKI Qualified Certificates (currently Internet Draft)*

Note: See Annex D for further details of initial recommendation for the use of X.509 certificate fields to meet the requirements for Qualified Certificates

b) Profiles for supporting revocation checks using either:

- *X.509 Certificate Revocation Lists.*
- *On-line Certificate Status Protocol*

Note: It is considered that profiles for both solutions are required, as both solutions are likely to be widely adopted to meet differing requirements.

c) Profile for the use of the Lightweight Directory Access Protocol to access qualified certificates. Note that the PKIX draft Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2259) may meet this requirement.

d) Recommended algorithms and key lengths for certificate (CA) signatures: Current practice (e.g. Government of Canada Certificate Policy) suggest the DSA or RSA algorithm [ISO/IEC 14888-1, -3] with 1024 bits although for higher assurance 2048 bit keys may be necessary. The SHA-1 and RIPEMD-160 hashing algorithms [ISO/IEC 10118-3] are most widely recognized as being of acceptable strength for normal certificate periods. The acceptable algorithms and maximum key length changes with the introduction of new technology and techniques. So any recommendation in this area should be regularly (e.g. yearly) reviewed

e) Recommended signature algorithms and key lengths for end users. It should noted that in most cases the key pair has only to resist during the life time of the certificate, so shorter key sizes can be used

5.2.4 Certificate Policy and Practice Statements

A certificate policy is defined in X.509 as "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". The rules are commonly defined as part of the practice statement of a Certification Authority, but can also be stated as a collection of requirements, issued by a recognized authority, to be fulfilled by a Certification Authority (e.g. Certificate Policies for the Government of Canada Public Key Infrastructure)

In the context of the Directive, a common **Certificate Policy for CSPs issuing Qualified Certificates** could contain all the agreed common CSP requirements, for example the ones described in the previous section:

- Security Management
- Trustworthy systems
- Technical Profile
- Documentation of practice statement

A certificate policy may not only identify requirements on the CSP but also place obligations on the signer (for example keeping the secrecy of the private key). Recommendations for the use of certificates in supporting validation of electronic signatures may also be included in a Certificate Policy (see 4.9 for a more general discussion on policy issues).

A certificate policy is represented in the certificate by a unique, registered Object Identifier (OID). The registration process follows procedures specified in ISO/IEC and ITU standards. Only CAs conforming to this policy should use the OID of the policy in their certificates. The presence of a specific OID may thus be used to signify the certificate as being a Qualified Certificate as required in Annex I and II.

RFC 2527 (PKIX-4) provides a framework, in the form of an "outline", for such a certificate policy. Please note that it does not put up any specific requirements, other than that the document should follow the specified outline.

The advantage of using the RFC 2527 framework is that it enables subscribers, relying parties and evaluators to compare the stated policy with other policies that have been written using the same structure. It also covers nearly all the issues addressed in Annex II of the Directive (see annex C.2).

The following are examples of existing certificate policies that have been written using the RFC 2527 framework:

- Digital signature & confidentiality Certificate Policies for the Government of Canada PKI
- Swedish S-10 Certificate Policy for high assurance general ID-certificate with private key protected in an electronic ID-card
- Catalan Government Certificate Policy, based on Spanish bank standard TIBC smart card for private key and certificate storage.

A more concise form of the practice statement, which can be used to inform uses of the key points, is being developed by ICC in their project to develop a one-page Model PKI Disclosure Statement.

As discussed in section 4.6 signers and verifiers generally require recognition of a common or related certification policy. By establishing a certification policy for qualified certificates supporting qualified electronic signatures a common reference is provided for signer and verifiers. This certification policy would be based on use of the standards identified above.

***EESSI Requirement**: Standardized Certificate Policy for CSPs issuing Qualified Certificates.*

5.2.5 Conformance Assessment

It is currently unclear how conformance assessment of trustworthy systems (Annex IIe) shall be performed, since this is not mentioned in article 3.2b of the Directive. However, it can be assumed

that this also should be performed by appropriate public or private bodies, similarly to secure signature creation devices.

Voluntary certification of CSP issuing certificates can be carried out within a general framework as described in 5.1.5.

For qualified electronic signatures, conformance assessment of the following additional requirements may be required:

- Additional Security Management requirements for CSPs supporting Qualified Electronic Signatures (see 5.2.1),
- Requirements on the use of trustworthy systems (see 5.2.2)
- Technical Profile for Qualified Electronic Signatures (see 5.2.3)
- Requirements for the publication of Certificate Practice Statements (see 5.2.4)

EESSI Requirement*: Agreement on conformance assessment requirements for CSPs issuing qualified certificates.*

5.3 CSPs Issuing Trusted Time-Stamps

It is often important to get an independent time-stamp associated with an electronic signature. This may be needed to meet requirements for timing an event in support of application of electronic signatures (e.g. time of contract), but is also necessary to counter certain threats associated with the use of electronic signatures supported by public key certificates, as described in section 4.2.

5.3.1 Security Management

Nearly all the requirements for security management of a time-stamping service would be addressed through adoption of a general security management standard such as BS 7799. Clock precision is of specific concern. Also, particular consideration will need to be given to service availability and integrity.

EESSI Requirement*: Security Management requirements for CSPs issuing Trusted time-stamps*

EESSI Initial Recommendation*: BS 7799 equivalent with special controls for clock precision.*

5.3.2 Use of Trustworthy Systems

The use of trustworthy system and products is necessary for CSP issuing trusted time-stamps, as for other CSPs. Thus, it is suggested that the same requirements apply as discussed in 5.1.2.

EESSI Requirement*: Requirement for use of trustworthy systems and products by CSPs issuing trusted time-stamps*

EESSI Initial Recommendation: *As in 5.1.2.*

5.3.3 Technical Profile Requirements

An Internet draft is under development (draft-ietf-pkix-time-stamp-01.txt) which may be used as the basis for a technical profile.

EESSI Requirement*: Technical Profile for CSPs issuing time-stamps.*

EESSI Initial Recommendation: *Endorsement of the RFC resulting from the development of the Internet draft Internet X.509 Public Key Infrastructure Time Stamp Protocols draft-ietf-pkix-time-stamp-01.txt.*

5.3.4 Trusted Time-stamping Service Policy and Practice Statements

CSPs issuing trusted time-stamps should operate within a defined policy, which may be published by the CSP as a practice statement in a similar way similar that certification practice statements relate to certificate policies.

***EESSI Requirement**: Standardized Policy for CSPs issuing Trusted Time-stamps.*

5.3.5 Conformance Assessment

Conformance assessment of CSP issuing certificates can be carried out within a general framework as described in 5.1.5.

For qualified electronic signatures, conformance assessment of the following additional requirements may be required:

- Requirements on the use of trustworthy systems (see 5.3.2)
- Technical Profile for CSPs issuing time-stamps (see 5.3.3)
- Requirements for the publication of Certificate Practice Statements (see 5.3.3)

***EESSI Requirement**: Agreement on conformance assessment requirements for CSPs issuing trusted time-stamps.*

5.4 Other CSPs Services

This may include:

- Attribute Authority services
- Trusted Archival services
- Notarisation services

The standardization requirements in these areas require further study.

***EESSI Requirement**: Study of the requirements for CSPs supporting notarisation services.*

***EESSI Requirement**: Study of the requirements for CSPs supporting trusted archival services.*

***EESSI Requirement**: Study of the requirements for CSPs issuing attribute certificates.*

6. Functional and quality standards for signature creation and verification products

Article 3.5: The Commission may, according to the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic signature products in the Official Journal of the European Communities. Member States shall presume compliance with the requirements laid down in point (f) of Annex II and Annex III when an electronic signature product meets those standards.

The following conclusions can be drawn from this article:

- There is a need for the development of one or more specifications for «secure signature creation devices», fulfilling the requirements in Annex III. Products conformant with these standards can be used to create qualified electronic signatures.
- Although Annex III only covers requirements for the creation device and not the entire signature process and environment (according to preamble 8a), it is useful to consider also the operating environment of the device, its user interface and, maybe most importantly, user behaviour. There may therefore also be a need for a specification that also considers these aspects. Products conformant with such a standard will thus enhance the requirements for the baseline.

Article 6: Member States and Commission (shall) work together to promote development and use of signature verification devices, in the light of the recommendations in Annex IV and in the interest of the consumer.

The following conclusion can be drawn from this article:

- There are no formal requirements for signature verification; annex IV only gives recommendations. However, there may also be a need for a specification for the signature verification procedure, including both the products used for verification, and their management.

This chapter describes the requirements for functional and quality standards for signature creation devices, the signature creation process and the signature verification process, according to Level 3 of the standardization framework model. It also describes the corresponding required conformity assessment procedures.

6.1 Signature creation devices

6.1.1 Requirements for secure electronic signature creation devices

Annex III describes the requirements for secure electronic signature creation devices. A standard is needed, that describes the requirements to fulfil Annex III in detail. Conformity assessment (either through voluntary certification or manufacturer's declaration) can then be performed against this standard.

The following table describes the requirements on signature creation devices, as specified in Annex III, and the conclusions when using current digital signature and public key certificate technology.

Requirement	Conclusion
1. Secure signature creation devices shall at least ensure, by appropriate technical and procedural means, that	The device shall support the following requirements:
(a) the signature creation data used for signature generation can practically occur only once, and that its secrecy is reasonably assured;	1. The key generation mechanism (either inside the device, or at the CSP) shall be based on a good random or pseudo-random number generator, to avoid two users may getting the same key pair. 2. The storage mechanism for the private key shall be well protected against outside access threats. 3. It shall not be possible to reproduce or make a copy of the private key, or of the whole device including the private key (see the note below).
(b) the signature creation data used for signature generation cannot be derived with reasonable assurance and that the signature is protected against forgery using currently available technology;	4. The cryptographic algorithm and key length must be strong enough to resist calculation of the private signature key from the public signature key or from the signature itself, at least during the whole validity period of the corresponding certificate. 5. The hashing algorithm must be strong enough to resist preparing a message with a given hash value, a second message with the same hash as a first message, or a pair of messages with the same hash value
(c) the signature creation data used for signature generation can be reliably protected by the legitimate holder against the use of others.	6. The use of the private key shall be protected by a password (passphrase or PIN code), resistant to common attacks (e.g. cannot be found using a dictionary of commonly used words). 7. There shall be a mechanism to prevent «exhaustive search» for the correct password.
2. Secure signature creation devices shall not alter the data to be signed nor prevent that those data are presented to the signatory prior to the signature process.	8. (No further consequence can be found for this requirement.)

Note on item 3: There are different interpretations of the requirement «occur only once»; thus item 3 is not an agreed interpretation. If the key shall only occur once, it may mean that it shall not be possible to make a copy of the key, even for backup purposes. The key must then be stored in a tamper-proof device. Furthermore, it implies that the private key could never leave the device, which means that the signature generation is done within the device. On the other hand, “occur only once” may only mean that the probability of two users’ private keys having the same value should be sufficiently low.

Note on item 8: This raises the question on whether or not the presentation of the data to be signed must be presented by the "secure signature creation device" and whether the presentation shall be done securely. The answer in the Directive is left open.

Presently, the most common and accepted technology for implementing a secure electronic creation device with the above requirements is a smart card used together with a Card Acceptor Device (card reader). The smart card contains the «signature creation data», i.e. «the private cryptographic key which is used by the signer in creating an electronic signature», protected by a PIN code. The private key can not be read out, a blocking function prevents exhaustive search for the correct PIN, and the smart card can not be copied. Other hardware tokens, such as a PCMCIA card, a mobile phone with a SIM card or a Personal Digital Assistant, can offer similar level of protection.

Currently, a PIN or a password is usually employed to protect the private key, and ensure that only the legitimate key holder has access to the key. Biometric identification would be a more secure and user-friendly way of authentication the key holder. It can be expected that biometrics, and especially finger print identification, in the near future will replace the use of PIN and passwords for this purpose.

There are differing opinions amongst experts if a hardware token is needed to fulfil the minimum requirements of Annex III or not. The EESSI expert team does not make any judgement on where the minimum level is. We only state that if a hardware token is used, the requirements of Annex III can easily be fulfilled. However, conformance with specified security requirements and evaluation standards like ITSEC or Common Criteria may also by used to meet these requirements. Thus, a standard or profile is needed to provide detailed specifications for these requirements.

Examples on private key protection requirements and standards

The German regulation requires ITSEC E4 HIGH for key generation and private key protection in the smart card. For the «signing environment», they require E2 HIGH for private use and E4 HIGH for public/commercial use.

The Italian regulation requires ITSEC E3 HIGH for key generation and private key protection. It is unclear if this requirement also encompasses the signing environment.

The Swedish S10 Certificate Policy only requires that the private key is stored in a smart card, with general security requirements, without requiring a specific assurance level.

The Canadian Government Certificate Policy requires FIPS 140-1 Level 1 for the cryptographic module for medium-level assurance and Level 2 for high-level assurance. The first can be implemented in software but the latter can only be implemented in a smart card or in a secure operating system.

The European Smart Card Industry Association (Eurosmart), which consists of 13 leading suppliers, has recently developed and registered a «Protection Profile for Smart Cards with Embedded Software». The protection profile is based on the Common Criteria for Information Technology Security Evaluation. Visa has recently published a similar draft of a Smart Card Protection Profile.

***EESSI Requirement**: Specification of security requirements for hardware tokens used as secure signature creation devices*

***EESSI Initial recommendation**: Use of hardware tokens conforming to any of the following specifications: Eurosmart PP/9809, a suitable ITSEC security level and target, or FIPS 140-1 Level 2.*

6.1.2 Conformity assessment of secure signature creation devices

Article 3.4: The conformity of secure signature creation devices with Annex III is determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9 (the Committee), establish criteria for Member States in determining whether a body is appropriate to be designated. Determination of conformity with the requirements of Annex III made by these bodies shall be recognized by all Member States.

Article 3.5: The Commission may, according to the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic signature products in the Official Journal of the European Communities. **Member States shall presume compliance with the requirements laid down in point (f) of Annex II and Annex III when an electronic signature product meets those standards.**

This means in practice that:

- The Commission shall establish criteria for the "notified bodies" which shall perform conformity assessment. These criteria may for example be based on EN 45011 (Certification Bodies for Products). These bodies can either be assessed and accredited by a nationally recognized accreditation body, or by another appropriate body designated by the Member State.
- Also, the Commission shall publish reference numbers of standards for products meeting the requirements of Annex III (see previous section).

The article thus states that the Member States may put in place a scheme for assessment of conformity with Annex III and the pursuant standard(s).

EESSI Requirement*: Specification of criteria for evaluation bodies performing conformity assessment of secure signing devices.*

EESSI Recommendation: *If existing security standards are used, as recommended in the previous section, existing accreditation and certification schemes can be used.*

6.2 Signature creation process and environment

Preamble 15: Whereas Annex III covers requirements for secure signature creation devices to ensure the functionality of advanced electronic signatures; whereas it does not cover the entire system environment in which such devices operate;

The secure signature creation device is only a part of the total environment needed to create a signature. In addition, there is a need for a specification, which not only considers the requirements on the signature creation device itself, but the whole signature creation process, and the signature creation environment.

For a supplier, using such a specification to develop products would be voluntary. For a signer, to use a product developed according to such a specification would be a voluntary enhancement to the electronic signature requirements.

Note: Currently, electronic signatures are mostly only applied to textual information. However, nothing in the Directive makes any such limitation, and any standard for electronic signatures should cover signatures for any type of multimedia information, such as pictures, sound and video, and combinations of these.

6.2.1 User interface for signature creation

The following are examples of requirements that could be considered:

- The signer shall be able to (and required to) verify the content of the data intended to be signed. The signer may even be forced to review the whole information to be signed, whichever media it is based on (text, audio, video).

- The signer shall be informed by the implications of his signature with a suitable message (e.g. describing the rules he will accept by affixing the signature).
- The signer shall perform a «wilful act» when signing, for example by entering his PIN or password for every signature. Clicking on a button may not be enough, both for the «wilful» reason and for security reasons.
- When receiving the device, the user must be informed in writing of, and agree to, the rules of its use (not writing down the PIN code, reporting when the device is stolen or lost etc). This requirement is usually enforced through a contract between the end-user and the issuing organization.

***EESSI Requirement**: Specification of user interface to signature creation products.*

***EESSI Initial recommendation**: Adoption of the above set of requirements.*

6.2.2 Operating environment and management

Several possible configurations for the signing environment can be envisaged, for example:

- Smart card, secure Card Accepting Device with keyboard and display
- Smart card, CAD with keyboard (data displayed on PC)
- Smart card, CAD (PIN input and data display on PC)
- Secure signing server containing private keys, accessed via a secure channel which authenticates the user.

For the operating environment and its management, only guidelines can be provided, since this also involves the user, his environment and his management of that environment.

***EESSI Requirement**: Guidelines for the operating environment of signature creation and its management, for different signature device environments.*

6.2.3 Conformity Assessment of user interface and signature creation environment

It may be possible to assess conformity of the user interface to the signature creation environment. However, conformity assessment of the whole signature creation environment is not possible, since such a standard only will include guidelines involving the user.

6.3 Signature verification process and environment

Signature verification is a process which 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 uses the text «displayed to the verifier», which might be interpreted as verification by a natural person. Only this first case is considered below. 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 information may use any type of media (text, sound, video etc).

6.3.1 Recommendations for signature verification

For signature verification, only recommendations are laid out in Annex IV of the Directive. A specification is needed, which describes in detail how to fulfil the recommendations in Annex IV. The following table describes the recommendations as specified in Annex IV, and the conclusions

from these recommendations when using current digital signature and public key certificate technology.

Recommendation	Conclusion
During signature verification process it should be ensured with reasonable certainty, that	The signature verification process shall support the following requirements:
(a) the data used for verifying the signature correspond to the data displayed to the verifier;	1. The information which is used for verifying the signature shall be correctly presented to the verifier (see note 1).
(b) the signature is reliably verified and the result of that verification is correctly displayed;	2. The mathematical verification of the signature is done correctly. The verifier is notified clearly of any errors.
(c) the verifier can, as necessary, reliably establish the contents of the signed data;	3. The contents of the message shall be presented correctly.
(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified, and that the result of verification and the signatory's identity are correctly displayed and the use of a pseudonym must be clearly indicated; and	4. The certificate chain must be validated. 5. Revocation status must be checked. 6. Signature and certificate chain must be time-stamped (See note 2 below). 7. The signer's identity must be displayed, and any use of pseudonym must be indicated.
(e) any security relevant changes can be detected.	8. Any integrity violation (i.e. change in the content of the signed message) shall be indicated.

Note 1: The signature verification process thus consists of a number of steps and measures that need to be taken in order to completely verify the signature. The possible failure at each step needs to be presented to the verifier.

All relevant information from the signature verification should ideally be available for the verifier to inspect. The following is a tentative list of such items:

- Signer's identity, as described by all relevant naming attributes contained in the certificate
- Type of commitment, if indicated by the signature policy
- Validity period of the certificate
- Certificate policies indicated in the certificate
- Any specified limitation of the usage of the certificate, or the value of the transaction
- Issuer's identity, as described by all relevant naming attributes contained in the certificate
- Revocation status information of the certificate
- Corresponding information for all CA certificates in the certificate chain
- Indication of root certificate used for verification of the certificate chain

Such an inspection by a verifier would be practically impossible because it would take too long and because most verifiers would not be in a position to verify all the items themselves. In order to satisfy this requirement, it may be possible to states against which *named set of rules* the

electronic signature has been verified and thus limit the display to the name of the set of rules, i.e. the name of the signature policy.

Note 2:

The verification of a signature can occur at a significant period after the signature creation time, and hence the verifier's current revocation information may not be applicable to the time of creation. In order to verify the validity and the authenticity of the certificate used by the signer at the time of the signature, it must be proven that that certificate existed and was valid, i.e. not revoked, at that time.

The practical way to prove, both at the time of the first verification and at the time of a later verification, that the signer private key was used during the operational period of the certificate is to time-stamp the signature of the signer by obtaining a time-stamp from a Time Stamping Authority (TSA). This should occur as soon as possible after the signature was created. In this way, an early comparison can be made between the revocation information, as indicated by the Certification Authority from the signer, and the time as indicated by the TSA. If the time indicated by the TSA falls within the operational period of the certificate, and is earlier than the revocation time of the certificate, then the signature was indeed done during the operational period of the certificate, and should be declared valid. If not, the signature should be declared as invalid.

Time-stamping can then be considered as a requirement for the verifier to later prove that the signature was valid. The time-stamp can either be obtained by the verifier himself, or provided by the signer. However, all signature verification issues are recommendations, and can thus be regarded as part of the electronic signature enhancements.

Another means of supporting long term validation of electronic signatures is through the support of trusted archival services. Such a service can maintain a record of the existence and validity of electronic signatures near the time that they were created which can later be used as evidence a long time later.

EESSI Requirement*: Specification of signature verification procedures fulfilling the requirements of Annex IV, including what to display to the verifier.*

6.3.2 Conformity Assessment of signature verification products

Conformity assessment of signature verification products is not possible, since the standard only will be a set of guidelines. The only thing possible is a manufacturer’s declaration that his product is following the published guidelines.

7. Interoperability standardization requirements for Electronic Signatures

The following sections identify various topics that need to be addressed mainly for interoperability reasons. In some cases, **standards** are identified, while in some other cases, the need for further **studies** is highlighted. Such studies could be sponsored by the European Community, e.g. as part of the IST Fifth Framework Programme or the ISIS Programme.

7.1 Data format definitions

7.1.1 Electronic Signature syntax and encoding formats

In order to support the interoperability of electronic signatures it is necessary to standardize their format. This is what is referred to in ISO/IEC 13888 as "non-repudiation token". This means that both the syntax and the encoding of an electronic signature have to be defined. The format is limited to the use of certificate-based digital signature techniques to construct and verify electronic signatures. Unless such a standard is established, a proliferation of various formats will be observed.

The simplest case of electronic signature involves a single electronic signature over a document. While this was necessary, it is insufficient in many applications when a contract must be signed by at least two persons. There are many ways to support multiple signatures by embedding, concatenating or making use of both techniques. Standards are needed in this area.

Signatures also need to be done by individuals acting on behalf of their company. Thus signatures under a role need to be considered.

Standards are in the final stages of drafting in the IETF for applying digital signatures to electronic mail. This consists of a basic structure which can be used for signing any data object, called Cryptographic Message Syntax (CMS), and an adaptation of this to the encoding syntax used in electronic mail called S/MIME (Secure MIME – MIME being the general encoding structure used for Internet mail). Earlier versions of these standards are already widely implemented.

The CMS standard provides tools, which can be used to encode qualified electronic signatures. However, they currently do not define the use of services such as time-stamping considered necessary for electronic signatures which can be independently validated over long periods (e.g. to an independent adjudicator).

Recently, the World Wide Web Consortium (W3C) has founded a joint Working Group with the IETF. The mission of this working group is to develop an XML compliant syntax used for representing the signature of Web resources and portions of protocol messages and procedures for computing and verifying such signatures.

An ETSI working group is already actively working in the definition of the core constituents of an electronic signature which can be validated after long periods. The end-result of this work is to allow adjudicators or other parties to use a common tool to verify the validity of an electronic signature against a signature policy.

A draft report of the ETSI work can be found at: http://www.etsi.org/sec/el-sign.htm

EESSI Requirement: *Specification of the syntax and encoding format of an Electronic Signature, including support for multiple signatures and roles.*

EESSI Initial Recommendation*: The CMS and S/MIME data structures can be used to meet the basic requirements of electronic signatures. However, to meet the requirements of enhanced electronic signatures that can be validated over a significant period, further steps are necessary. A draft addressing this matter is being prepared by the ETSI TPP working group, a sub-group from the ETSI TC Security which is aimed at meeting this requirement building on CMS. Pilots*

experimenting with this new format would help to validate it. In the IETF community two independent implementations are needed before publishing an RFC standard. In the same way, two independent pilots should be realized before publishing such a standard as an ENV.

7.1.2 Qualified Certificates

The primary structure to be specified is the " Qualified Certificate " mentioned in the draft Directive. X.509 or PKIX certificates in their standard form can accommodate the various items, with the exception of the three requirements listed below :

Annex I: Qualified certificates must contain:
(a) an indication that the certificate is issued as a qualified certificate ;
(c) the name of the signatory or a pseudonym which shall be identified as such ;
(j) limits on the value of transactions for which the certificate can be used, if applicable.

Initial recommendations for the use of X.509 certificates as qualified certificates and on possible ways to address these three requirements are given in Annex D of this report.

Some work has already been initiated at the IETF on the topic of " Qualified Certificates ", especially regarding naming standards. However, it is unlikely that all the requirements from the Annex I are going to be fulfilled by that work.

EESSI Requirement*: Standard for the use of X.509 public key certificates as qualified certificates.*

EESSI Initial Recommendation*: Support of the on-going work in IETF PKIX in this area, and progress work on European specific aspects that are not addressed by the current PKIX qualified certificates working draft.*

7.1.3 Other data structures

There is a requirement to define profiles also for:

- Certificates Revocation Lists (CRLs),
- Authority Revocation Lists (ARLs),
- OSCP responses (obtained through the On line Certificate Status Protocol),
- Time-stamps (obtained through the Time Stamping Protocol),

In addition, a definition and profiling of Attributes Certificates is also needed.

A draft addressing this matter is being prepared by the ETSI TPP working group, a sub-group from the ETSI TC Security. Attribute Certificates are being defined both by ISO and the PKIX working group.

EESSI Requirement: *Profile for Certificates Revocation Lists (CRLs), Authority Revocation Lists (ARLs), OSCP responses and Time-Stamps.*

EESSI Initial Recommendation*: No specific recommendations can be made at this time.*

7.1.4 Signature policies

A commercial contract will have to refer to a signature policy which defines the way to verify the validity of the signature, i.e. whether the signature applied by the signer fulfils the rules applicable to the type of transaction that is being voluntarily agreed by the signer at the time he affixed his signature and which will then be used to verify the validity of the Electronic Signature. The correctness of the detailed terms of the contract contained in the signed data is *not* part of this validation process.

Since the full definition of a signature policy may be quite large, it would be a waste of space to have it included in each signed document. What is required is an **unambiguous reference to a signature policy**. The format of such a reference would need to be standardized and would consist of a pointer to a signature policy (using e.g. a URL or/and an OID) and a hash of the signature policy to verify the integrity of the data fetched through the use of the pointer.

A further potential requirement is **the syntax and the encoding of the signature policy** so that an electronic signature can be automatically verified against the signature policy to which it refers.

Many applications currently only consider the case where there exists a single root CA so that it is possible to find a certification path to any CA. While this model may be adequate in some cases, it is limited. The main issue is that it mandates a model with a uniform trust which is quite impractical in the real world. A more general model would need to consider a direct *limited* trust with different CAs, where a given CA is only to be allowed to certify some name forms, and not others. Such constraints are normally present both in CA certificates (also called cross-certificates) and in self-signed certificates from root CAs and would need to be studied in more detail and then validated through pilot projects.

The signature policy should also take care of cross-certification aspects, indicating which certification paths may be used to validate a given certificate.

The signature policy identifies:

- the various root CAs that are trusted for a given type of transaction and *for what they are trusted*,
- the various certification paths that can be used (using naming constraints),
- the certificate policies, if any, that must be contained in the various certificates of a certification path,
- aspects that are relevant to time-stamping, e.g. by identifying the TSA (Time Stamping Authorities) that are pertinent for handling the type of transaction, and
- the conditions for the declaration and the publication of certificate revocations.

The indicated signature policy conditions will thus be used by the verifier to verify the validity of the signature.

A trust point refers to a CA usable as a start point to verify a certification path. In practice, it is a self-signed certificate from a CA. The replacement of that self-signed certificate (key rollover), its revocation or even the termination of activity of a CA will affect the corresponding trust point of the signature policies which then need to be updated. This problem needs further study.

EESSI Requirement*: Standard for reference to signature policies. Standard for description of the constituents of a signature policy so they can be made understandable both by a human being and a computer.*

EESSI Initial Recommendation: *A draft addressing these matters is being prepared by the ETSI TPP working group, a sub-group from the ETSI TC Security. Pilots experimenting this new format would help to validate it. Two independent pilots should be realized before publishing such a standard as an ENV.*

7.1.5 Definition and support of generic roles

The simplest case of a digital signature involves an individual, but without any further qualification. In the real world, many contracts are signed by people acting under a role in their organization or company: they sign under a role on behalf of their organization or company rather than for themselves. This is of particular importance for business to business transactions but also for business to individual transactions. There are two main ways to support roles:

- using claimed assertion of roles,

- by using **Attributes Certificates** or
- by role attributes within public key certificates.

All approaches have their advantages and their drawbacks.

Another variation of a person acting under a role, is when one person is given the right (e.g. through power of attorney) to act on behalf of another.

The support of roles has several implications. When Attribute Certificates are used, then the exact format of Attribute Certificates has to be specified (some work is being done in this area by the ISO / ITU work on further X.509 enhancements). In the last case, extensions to support roles in public key certificates have to be specified.

This is however not enough. Cross-border contracts have to relate to a common definition and understanding of the various practical roles used by contractual persons. Such a definition will have to be made by an international organization like the ICC.

EESSI Requirement**:** *An appropriate international organization should define generic roles that are relevant to current transactions or contracts so that they can then be included in either Attribute Certificates or Public Key Certificates as extensions.*

7.2 Repositories to support electronic signatures

7.2.1 Repository for certificate policies, signature policies and contract types

Certificate policies and signature policies are referenced by an OID. There is a need to have access to the human readable content of the policies, not only to estimate the quality of the service for issuing and maintaining the content of the certificate but also to understand the terms of the contract agreed by the certificate owner. Such information could be made available on trusted repositories in a standard form.

There are two ways to achieve this goal, either using a **central repository of certificate and signature policies** or **using a central repository of contract types** that will include the details of the policy.

These references will be given a unique reference number so that parties can incorporate them into electronic contracts. E-terms from the ICC (International Chamber of Commerce) might be a place to consider storing that information.

EESSI Requirement: *A repository of certificate policies, signature policies or of contract types is needed.*

EESSI Initial Recommendation*: The ICC (International Chamber of Commerce) repository being set up under the E-terms initiative could be used for such a purpose.*

7.3. Further studies

7.3.1 Scalable revocations

Repositories for CRLs are needed for all the certificates issued by a CA, unless an on-line status certificate server is provided.

Revocation has only been tested on some pilots with a small number of certificates. There have been few studies to anticipate situations with a large number of certificates and hence a large number of revocations. Some techniques have been recommended, as the use of delta-CRLs or of multiple distribution points with a partitioning of the CRLs. These techniques should be looked at either on a theoretical basis or an experimental basis.

EESSI Requirement*: More studies are needed on the way to handle large numbers of revoked certificates.*

7.3.2 Scaleable suspensions

Suspension is a particular case of revocation: it is a temporary revocation until it can be decided whether the certificate has to be revoked definitively or ceases to be temporarily revoked. While they are defined and described in the standards, suspended certificates have been very rarely considered in practice. The implications of the use of suspended certificates should be looked at in more detail. In particular, the use of suspended certificates may imply two time-stamps instead of one: one soon after the signature creation, i.e. during the suspension period and another one soon after the end of the suspension period.

EESSI Requirement*: More studies and explanations are needed on the way to handle suspended certificates in the context of their use in Electronic Signatures.*

7.3.3 Identification and naming

The topic of identification and naming needs to be addressed in order to allow a large deployment of a PKI. As the PKI naming information is to be computer processable the structure and allocation of names need to be more rigorous than currently existing for hand-written signatures. The main issue is that the subject identifier contained in a certificate may not be descriptive enough to unambiguously identify an entity. When dealing with this topic, it will be necessary to separate the case of identifiers assigned for organizations and for persons, i.e. employees from an organization or individuals.

Identifiers for organizations

An organization identifier is usually a *registered* name, i.e. business or trading name used in day to day business. This name is registered by a Naming Authority, which guarantees that the organization's registered name is unambiguous and cannot be confused with another organization. In order to get more information about a given *registered organization name*, it is necessary to fetch it from **a publicly available repository maintained by the Naming Authority**.

Identifiers for persons

The identifier may be a name or a pseudonym.

When it is a name, it is supposed to be descriptive enough to unambiguous identify the person. Two cases need to be distinguished: whether the name applies to a person from an organization (e.g. an employee or a member of an association) or to an individual citizen.

Person from an organization

Placing more attributes in the certificate may be one solution, for example by giving the organization unit of the person or the name of a city where the office is located. However, the more information placed in the certificate, the more problems arise if there is a change in the organization structure or the place of work. So this may not be the best solution. An alternative is to provide more attributes (like the organization unit and the place of work) through access to a directory maintained by the company.

Individual citizen

Placing more attributes in a certificate goes against privacy. In any case the Registration Authority will get information at the time of registration but all that information will not be placed in the certificate. The additional information may be placed in directory.

The basic question is how much information should be disclosed to allow to **handle homonyms** and to distinguish between persons having the same name and living in

the same city? Who should be allowed access to the additional information that is not included in the certificate? Under which circumstances?

When it is a **pseudonym**, the certificate does not disclose the identity of the person. However it ensures that the person has been correctly authenticated at the time of registration and therefore may be eligible to some advantages implicitly or explicitly obtained through the possession of the certificate.

***EESSI Requirement**: A specific study on solving name forms and name collisions both from a technical and legal point of view is needed. An extension to handle biometrics information in a certificate should also be specified. This topic is currently being partly addressed by the PKIX working group.*

7.3.4 Certification path validation

A certificate has to be validated using a self-signed root certificate and an appropriate certification path, composed of a chain of cross-certificates. A cross-certificate is a certificate issued by one CA to another CA (note that reciprocity is NOT implied).

The cross-certificate will only be issued after a proper examination of the CPS (Certificate Practice Statements) of the other CA and will indicate the conditions of use of such a certificate. Such conditions will be reflected both in the identification of certificate security policies but also in the naming constraints mentioned in the cross certificate so that applications can make use of them.

The issuance of such certificates and the way to use a chain of cross-certificates, ending at a self-signed certificate, containing either different policies or various naming constraints would need to be addressed. A better technical understanding of these issues is necessary, in particular before legislative actions may be taken in this area.

***EESSI Requirement**: More studies are needed to handle name constraints and certificate policy constraints in the verification of a certification path. The current PKIX part 1 (RFC 2459) document does not fully address this concern and an extension to that document should be studied and then proposed to the PKIX working group.*

7.4 Protocols to interoperate with CSPs

These protocols are usually classified into two categories: on one side the *management* protocols, e.g. to request the creation, renewal or revocation of a certificate and on the other side the *operational* protocols e.g. to request the retrieval of a certificate, a CRL or an on-line certificate status. Much work has already been done in this area by the IETF, as it is the case for CAs, RAs, TSAs, Certificate Repositories, and On-line Certificate Status Providers. There are now so many options or variations that a profiling of the protocols needs to be done.

7.4.1 Operational protocols

7.4.1.1 Protocol to retrieve additional information from a repository

Currently the IETF has defined a standard that builds upon LDAP v2 (Lightweight Directory Access Protocol). The scalability issue raised before for CRLs might lead to the need of using the LDAP v3 protocol. This needs to be further studied.

Repositories for end-entity signature certificates are not strictly needed. The signer may include his signature certificate attached with every signed document.

However, repositories for cross-certificates are needed to verify a certification path, since it cannot be assumed that end-entities carry them along.

The most common form of certificate repository is a directory and the generally recognised standard for directory access is LDAP. The most widely implemented version of LDAP is v2 (RFC 1777), however, a new version of LDAP (v3) has been recently (RFC 2251). A specific use of LDAP v2 for accessing a certificate repository is defined in RFC 2559. Currently, no equivalent is defined for LDAP v3 although the differences from the view of supporting certificate repository requirements are not considered to be significant.

In addition, it may be useful to protect against the possible compromise of a CA key, should a compromise occur. In order to prove that a certificate, cross-certificate, CRL or ARL was produced by a CA before the compromise of its issuing key, it is necessary to time-stamp every element.

In such a case, not only the public key certificate from the signer - and the attribute certificate, if any is used - need to be time-stamped, but also each component from the certification path.

- Time-stamping the whole chain is one possibility. However, time-stamping every element (certificate, cross-certificate, CRL or ARL) when placed in the repository by the CA for the first time may be easier. In order to reduce the overhead, CAs could thus publish and maintain in an appropriate repository, time-stamped versions of every cross-certificate they issue. This will allow anyone to prove that a given cross-certificate was valid prior to the possible compromise of the issuing key of the CA. A combination of the two techniques could also be considered.

EESSI Requirement*: Standard for the access to a repository holding time-stamped certificates and scalable revocation information.*

EESSI Initial Recommendation: *Use of the LDAPv2 as defined in RFC 2559 or equivalent using the LDAP v3 protocol.*

7.4.1.2 Protocol to inter-operate with an on-line status certificate server

An alternative approach to checking whether a certificate is valid (e.g. not revoked) is to use an on-line service to check the validity of certificates. This provides a solution for the validation of electronic signatures which is easy for the verifier to support.

The IETF is drafting a standard protocol to access such as service called the on-line certificate status protocol (OCSP). The OCSP protocol being defined by IETF PKIX working group might need to be profiled.

EESSI Requirement*: Protocol for on-line certificate status check.*

EESSI Initial recommendation*: Use the Internet standard On Line Certificate Status Protocol to be published as an RFC in the near future. A profiling of the On Line Certificate Status protocol issued by the IETF may be needed.*

7.4.1.3 Protocol to inter-operate with a Time Stamping Authority (TSA)

It may be needed to re-verify the validity of a signed document years later after it has been signed, i.e. later validate the electronic signature. The certificates that were originally used may have all expired and some may have been revoked during their original operational period. Nevertheless it is still necessary to make use of them.

In order to re-verify the validity of a signed document years later after it has been signed, it is important to *reliably prove that all the certificates that are being used in the verification process were valid at the time the document was signed.* This may need to be done even:

- after the expiration of the certificate used at the time of generation of the signature,
- after one change of the certification key originally used to issue that certificate,
- after several changes of the certification keys from the chain of certificates to be used to validate the signature,

- after several changes of one of the self-signed certificates used to validate the certification path,
- after the time when the cryptography used is no longer secure, i.e. when it becomes possible to derive private keys from public keys, or to generate second time-stamp messages which use the same hash.

In order to re-verify the validity of a signed document years later after it has been signed, it is important to *reliably know that it was signed during the validity period of the certificates*.

The appropriate use of Time-stamps delivered by one or more Time Stamping Authorities is able to address these issues. A protocol to interoperate with Time Stamping Authorities is needed. Such a protocol is being defined within the IETF by the PKIX working group. The format of a Time-Stamping Token (i.e. a bit representation of a digital Time-stamp) is also part of this on-going work.

EESSI Requirement*: Protocol for access to a Time-Stamping service.*

EESSI Initial Recommendation*: Internet Draft Time Stamping Protocol (TSP). A profiling of the Time Stamping protocol under study by the PKIX working group may be needed, once this protocol will be published by the IETF.*

7.4.1.4 Notary functions and protocols

In many cases the recipient of an electronic signature will first verify that electronic signature and then keep some elements for a later proof. This may be sufficient for many applications.

For some other applications this may be insufficient for several reasons, in particular because a notary must affix its own signature after the proper *verification of the content* of the document already signed by the two parties. A notary is also supposed to *store* the end result and make that content available upon request.

EESSI Requirement: *Study is required to identify the role of notaries in an electronic world both from a technical perspective and a business perspective..*

7.4.2 Entity registration protocols

These protocols are not visible to a verifier. So they do not impact interoperability between a signer and a verifier or between a verifier and a TSP. However, some of the currently defined protocols suffer from some limitations.

There are many ways to register to a Registration Authority in order to obtain later a certificate from a CA. This is because the key can be generated in multiple places and can be protected using multiple ways. The IETF has standardized basic protocols allowing remote registration that suffer from some problems; in particular the main issue is that a secret must be exchanged *in advance* with a Registration Authority *using "out of bands" means*. This is restrictive and more flexibility should be given.

EESSI Requirement: *Additional registration protocols should be defined to allow registration without the need to exchange a secret by out-of-bands means. In addition registration protocols for smart cards and in particular smart cards able to internally generate the key pair should be considered. This work could be done either by the PKIX working group or by ISO.*

7.5 Smart cards and other hardware tokens

Smart cards, personal digital assistants and other hardware tokens are regarded as ideal to protect private keys, to store certificates, to carry trust point references and to carry signature policy references. Some publicly available specifications like PKCS#11 are being used to allow some form of interoperability but more standardization would be needed in the area of the use of smart

card or other hardware tokens for storing other information. Smart cards are currently dealt with in several groups, like in ETSI (SMG 10), in CEN (TC 224 and TC 251) and in ISO/IEC SC 17. Vendor-specific standards are being used for personal assistants.

7.5.1 Use of hardware devices for signature creation and storage of other security related information

Mobile users should ideally carry private keys, certificates and the various signature policies they use in their smart cards, personal assistants or other types of hardware devices. However, for security reasons, it is not sufficient only to use the hardware device as a storage medium. The device must also be able to create the digital signature without disclosing the private key. To achieve this with vendor independence and interoperability between products, a standard is needed for using various hardware devices for the storage and usage of private keys, as well as the storage of other PKI objects.

Signature policies, which are likely to be too large to carry within a card, could be carried by references (e.g. OIDs and/or URLs and hash). Such a signature policy enables the conditions needed to validate the electronic signature to be clearly identified.

In Germany, DIN has recently published "Vornorm 66291-1: Specification of chipcard interface with digital signature application/function according to SigG and SigV (DIN NI-17.4)". This specification defines the interface between a interface device (a PC and/or a terminal) and a digital signature card, which is in compliance with the German digital signature law. The specification takes into account the German legal regulations and relevant standards for smart cards (especially ISO/IEC 7816).

Internationally, a number of companies have agreed on the PKCS#15 publicly available specification for storage of security related information on smart cards. The standard has been published by RSA Labs and is also proposed as the subject of a new work item in ISO/IEC JTC1/SC17. However, PKCS#15 presently covers only the storage of security objects. Usage of the private key may be performed either according to ISO 7816-8 or using a proprietary commend. Here there is a need for further standardization.

EESSI Requirement: *A standard for storing and using private keys and other PKI objects on smart cards or other hardware devices is needed. The PKCS#15 publicly available specification and the DIN Vornorm should be studied to make sure they fulfil these requirements.*

7.6 Application Programming Interfaces (APIs)

APIs allow programmers to use a function by knowing only the interface to the function without the need to know the details of the function itself. Two basic set of APIs are needed to be either both defined and experimented (7.6.1) or only experimented with (7.6.2).

7.6.1 APIs for infrastructure independence

The IETF has defined both management and operational protocols to interface with a PKI but no APIs to invoke these protocols. In order to allow programmers to have an easy access to any PKI infrastructure conforming to the PKIX protocols, APIs interfacing these protocols would be most useful.

EESSI Requirement: *There is a need to define APIs on top of the IETF operational and management protocols so that access to various PKI infrastructures conforming to the PKIX protocols can be made easier for implementers.*

7.6.2 APIs for generating and verifying electronic signatures

ETSI is currently defining a format for "Electronic Signature Tokens". An API to manipulate these tokens has already been defined by the IETF, but got an informational status due to a lack of implementations. There also exist commercially available APIs for the generation and verification of electronic signatures, such as Microsoft Crypto-API and Intel CDSA. However, these APIs can only be used for the generation of “raw” PKCS#7 signed messages; they do not consider all the requirements of an electronic signature. Since ETSI should now shortly provide a format, it is the right time to start experiments and for pilots to use that format and support the generation and verification of electronic signature tokens based on the document issued by the IETF, i.e. Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API) (RFC 2479).

EESSI Recommendation: *There is a need to experiment the IDUP APIs in at least two pilots in conjunction with a standard format for electronic signatures in order to test both portability and interoperability.*

8. Recommendations and Outline of Proposed Work Programme

This section first identifies the co-ordination needed at an international level, and then identifies the organizations concerned by the practical deployment of electronic signatures. Then it considers the various work areas and for each one tentatively assigns one or more organizations able to take on that work area. Finally, each organization is provided with its own list of work areas.

8.1 International co-ordination and promotion

The work programme proposed below by EESSI is mainly focused on quickly reaching agreement at a European level to support the implementation of the Directive. However, it is paramount that the agreements and standards that are proposed already have, or can get, international acceptance outside Europe.

For this reason, all work initiated by EESSI should, to an extent as large as possible, take into consideration current international standardisation and be performed in consultation with other international organizations.

In some cases, standards will still have to be developed in the framework of European standardization bodies or industry fora, due to the lack of international agreement in this novel area. However, such standards and agreements should as quickly as possible be internationally promoted and proposed as work items in the relevant international standards bodies.

Presently, work related to Electronic Signatures is performed in specialized working groups of many international organizations, other than those involved in EESSI (IETF, ISO, ITU, W3C, ICC, UNCITRAL, ABA to name a few). Some of these are studying technical aspects, others are studying business, legal and policy aspects.

In order to co-ordinate and promote international activities in the area of electronic signatures, EESSI proposes:

- The "Electronic Signature Committee", which is composed of representatives of the Member States and the Commission would need to get advice from the industry. To this respect, EESSI recommends the establishment in due course of an " Electronic Signature Industry Advisory Group" to provide advice and recommendations to the "Electronic Signature Committee". The "Electronic Signature Industry Advisory Group" should be composed of recognized technical experts in the area of electronic signatures from the vendor and user industry.
- The arrangement of an ”International Electronic Signature Forum”, where representatives from those different organizations can meet and co-ordinate their activities. The Forum should be arranged on an event basis, involve users and regulators as well as providers of products and services, rather than an ongoing activity.
- Presentation of EESSI work programme to the technical and steering committees of the relevant European and international bodies (CEN, ETSI, PKIX, ISO, ITU-T, ICC).
- Presentation of EESSI to those national institutions presently in the process of drafting legislation on electronic signatures (possibly initiated through SOGITS).
- Participation and presentation of EESSI at international conferences and events (e.g. ISSE 99, RSA 2000, ABA).

8.2 Organizations involved

This section lists the organizations that can contribute to the deployment of electronic signatures. The following standard bodies and other organizations have been tentatively considered:

- CEN

- ETSI
- European co-operation for Accreditation (EA)
- ICC
- Open Group
- IETF
- ISO/IEC JTC1/SC 27

From the formal European standardization perspective, the work programme should be executed within CEN and ETSI. In general, ETSI is standardizing the network infrastructure and CEN the applications for the information society.

The activities on electronic signature standardization in both these groups should be open to participation from all industrial sectors with interests in supporting or using electronic signature products and services.

It is proposed that the CEN work be carried out initially in CEN/ISSS Workshops, resulting in CEN Workshop Agreements (CWAs), subject to the detailed arrangements being laid down in the relevant Workshop Business Plans. For ETSI, the work can be carried out in the existing TC/SEC, resulting in ETSI Standards (ES) and/or formal European Standards (EN). If it proves necessary for individual topics, for instance where in defining the work item scope there is a very substantial common interest, joint open Workshop-type arrangements could be made, subject to agreement between the two bodies on the operational rules. In any case, it will be necessary to ensure the right liaisons at the working level, and, initially at least, through the continuance of the EESSI mechanism under ICTSB at the policy level.

For some work areas, it is proposed that formal European Standards will be needed ultimately, partly to achieve an appropriate maintenance process. These can be prepared using already adopted CWAs or ETSI standards, or directly in the ETSI case; in CEN's case it would be necessary to create a new Technical Committee for this purpose, although this would take some time. However, the entry into force of the Directive is still some way off, and nothing precludes the initial use of CWAs.

Regarding the work to be performed in IETF PKIX, the European presence and involvement in the relevant IETF working groups, such as PKIX, is presently quite small. All involvement in IETF is on a personal basis, but all industry and European organizations must be stimulated to actively involve themselves in such activities.

8.3 Description of work areas

Below, all identified work areas are described, with priorities and proposed responsible body indicated. The rationales for the different priority classes are the following:

Urgent	These activities are on the "critical path" for the meeting the requirements identified by this report. The results of these work areas are either needed before other areas can be concluded, or need to be finished early, in order to give potential suppliers the necessary lead-time to develop compatible software and hardware products for qualified electronic signatures in time for the entry into force of the directive. If these critical areas are not addressed urgently, it would have a wide impact on the general provision of products and services for electronic signatures.
High	The results of these work areas are also needed for implementation of products and services for qualified electronic signatures compliant with the directive.
Medium	The results of these work areas are needed for general electronic signatures and to achieve greater interoperability, but are less critical than the high priority areas.

Low These areas should be addressed on a longer term.

For high and medium priority items, the required target date is also specified as T0 + xQ, where T0 is the earliest date that work can start. All items are given an alphabetic label to enable easy reference.

Since a large number of standardization activities now will initiated and carried out by various bodies, there is a requirement for technical co-ordination between these activities to ensure:

- that boundary issues between different areas are properly addressed (e.g: Shall the requirements related to device personalization be addressed in the CSP policy or in the standard for creation devices?)
- that a consistent system-wide security is achieved. This should be supported by a system-wide protection profile and security threat analysis.
- that the work plan can be adapted to changes in technologies and market priorities.

A. First set of components, fulfilling the framework for qualified electronic signatures.

This work area comprises the specification of a first set of components, fulfilling the requirements of a framework for qualified electronic signatures [4.3]. The specification will contain references to existing technical standards and mechanisms. The work thus only involves the selection of suitable standards to use. One or more of the selected components may later be exchanged with other standards and/or mechanisms, forming new sets of components.

This work is necessary as the basis for several of the other work areas, since it will define a first set of mechanisms to be used. It thus needs to be started in advance of the other activities. It is recommended to undertake this work as a joint CEN-ETSI effort with a **urgent priority**, and a target date of T0 + 2Q for a first delivery. This work may then need to be continued as an ongoing activity. The results may be published as a CWA and/or an ETSI standard.

8.3.1 CSP Management and Policy Issues

B. General CSP Security Management

This work area comprises specifications and general guidance for the security management for CSPs supporting Electronic Signatures. It shall allow for technology neutrality but provide guidance to CSPs to ensure that a basic level of quality in the provision CSP services can be achieved, through adoption of recognized codes of practice for security management and the publication of the practices adopted by the CSP.

EESSI Requirements to be addressed by this work area are:

- European recognition of standard security management guidelines (e.g. BS 7799, ISO TR 13335, COBIT) generally applicable to CSPs supporting electronic signatures. [5.1.1]
- European recognition of Specific Requirements for Assessment of Security Management (e.g. as in BS 7799 part 2) generally applicable to CSPs supporting electronic signatures.[5.1.1]
- General requirements for use of trustworthy systems and products by CSPs. [5.1.2]
- Requirements for the documentation of CSP practices and policies (this may be based on BS 7799 requirements for documentation of policies). [5.1.4]
- General conformance assessment scheme for CSP. [5.1.5]

It is recommended to undertake this work in a CEN Workshop with a **medium priority** with a target date of T0 + 2Q for the delivery of a CWA (Workshop Agreement).

C. Security Management and Certificate Policy for CSPs issuing Qualified Certificates

This work area shall provide a common policy identifying minimum essential requirements for CSPs issuing qualified certificates. Through the use of CSPs supporting this policy, users can be assured that the legal requirements of electronic equivalents to hand-written signatures are met. The specification is to be based on the framework defined in RFC 2527, filling in specific details to meet Directive requirements.

EESSI Requirements to be addressed by this work area are:

- Security Management requirements for CSPs issuing Qualified Certificates. [5.2.1]
- Technical Profiles for operational aspects of CSPs issuing qualified certificates. [5.2.3]
- Standardized Certificate Policy for CSPs issuing Qualified Certificates. [5.2.4]
- Agreement on conformance assessment requirements for CSPs issuing qualified certificates.[5.2.4]

It is recommended to undertake this work with a **high priority** in a CEN Workshop with a target date of T0 + 4Q for the delivery of a CWA (Workshop Agreement).

D. Specification of security requirements for trustworthy systems used by CSPs issuing qualified certificates

The purpose of this work area is to provide a set of requirements for the trustworthy systems used by CSPs issuing qualified certificates. The specification may be a combination of a Protection Profile based on Common Criteria and requirements for the cryptographic modules being used (FIPS 140-1 or equivalent). A new standard should preferably not be written, since this would cause an unacceptable delay in the development and deployment of such products.

It is suggested that the work area is combined with (F) below, and should contain the following activities:

- European recognition of FIPS 140-1 /adaptation of FIPS 140-1 as a European standard
- Selection of suitable FIPS 140-1 levels for signature creation devices and for cryptographic modules in trustworthy systems
- Adoption of existing Protection Profile(s) and/or ITSEC (use of Protection Profiles is preferred choice) security targets as security requirements for signature creation devices
- Possible development of a new Protection Profile for CSP systems issuing qualified certificates

It is recommended to undertake this work with a **urgent priority** in a CEN Workshop with a target date of T0+2Q for the delivery of a CWA (Workshop Agreement). Later, an international agreement or standard is needed.

E. Security Management and Policy for CSPs issuing Trusted Time-Stamps

This work area shall provide a common policy identifying minimum essential requirements for CSPs issuing time-stamps to enhance the security of electronic signatures.

EESSI Requirements to be addressed by this work area are:

- Security Management requirements for CSPs issuing trusted time-stamps.[5.1.1]
- Requirement for use of trustworthy systems and products by CSPs issuing trusted time-stamps [5.3.2]
- Technical Profile for CSPs issuing trusted time-stamps.[5.3.3]
- Standardized Policy for CSPs issuing trusted time-stamps
- Agreement on conformance assessment requirements for CSPs issuing trusted time-stamps.[5.3.5]

The policy for CSP issuing qualified certificates can be used as the basis for the development of this specification.

It is recommended to undertake this work with a **medium priority** in a CEN Workshop with a target date of T0 +4Q for the delivery of a CWA (Workshop Agreement).

8.3.2 Standards for Electronic Signature products

F. Specification of security requirements for hardware devices used as secure signature creation devices

The purpose of this work area is to provide a set of requirements for hardware devices protecting a private signing key and being used as signing device [6.1.1]. The work should only refer to existing and internationally accepted security standards and/or protection profiles. Another possibility is to provide a European acceptance of FIPS 140-1.

A new standard should not be written, since this would cause a unacceptable delay in the development and deployment of such products.

It is recommended to undertake this work with a **urgent priority** in a CEN Workshop with a target date of T0+2Q for the delivery of a CWA (Workshop Agreement). Later, an international agreement or standard is needed.

G. Specifications and guidelines for signature creation and verification products

The purpose of this work area is to provide specifications of functional and quality requirements of products for creation and verification of electronic signatures. The specifications should allow for technology neutrality but also provide guidance for specific technologies, such as smart cards and personal computers.

EESSI Requirements to be addressed by this work area are:

- Specification of user interface to signature creation products [6.2.1]
- Specification of the operating environment of signature creation and its management, for different signature device technologies [6.2.2]
- Specification of signature verification products and procedures [6.3.1]
- Requirements for the use of time-stamping and/or archival services to enable the use of electronic signatures as long term evidence [6.3.1]

There are no existing international standards in this field, only various national recommendations which need to be studied.

It is recommended to undertake this work with a **high priority** in a CEN Workshop with a target date of T0+4Q for the delivery of a CWA (Workshop Agreement) which later can be made into European prestandards (ENV).

8.3.3 Standards for interoperability

H. Electronic Signature syntax and encoding formats

The purpose of this work is to establish a standard format for electronic signatures, including support for multiple signatures and roles, to allow adjudicators or other parties to use a common tool to verify the validity of an electronic signature long after its initial use. This is a **high priority** item. A target date for a standard in this area is T0+2Q.

Since the ETSI TC security has already undertaken work in this area, it is recommended to support that work. A draft ETSI standard is expected before the end of this year. It could be then proposed for further processing as an EN.

I. Standard for the use of X.509 public key certificates as qualified certificates

The purpose of this work is to issue recommendations for the use of X.509 certificates as qualified certificates according to the Annex I of the Directive. This is a **urgent priority** item. A target date for a standard in this area is T0 + 2Q.

Work has already been initiated at the IETF on the topic of " Qualified Certificates ", and is expected to reach RFC status before the end of this year, but additional recommendations might be needed. However, further work will be necessary by ETSI in this area - perhaps in conjunction with CEN/ISSS - targeted at the specific requirements of the Directive that builds on the generic work of the IETF.

J. Standard for the profiling of CRLs, ARLs, OCSP responses and Time-Stamps

These data structures are defined in IETF standards. However, it might be useful to define some profiles in order to reduce the number of options and thus ease interoperability. This is a **medium priority** issue. The work of ETSI TC Security should address this requirement.

K. Use of smart cards for creating electronic signatures and Storage of other PKI objects

An internationally recognised standard is required for the use of smart cards for creation of electronic signatures and for storing other PKI objects, such as public key certificates and trust points. The publicly available specification PKCS #15 and DIN Vornorm may provide the starting points but this might need to be addressed in a de-jure standard within the scope of ISO/IEC JTC1/SC17. This is a **medium priority** item.

L. Additional protocols to interoperate with a repository

The scalability issue raised for CRLs might lead to the need of using the LDAP v3 protocol. This needs to be further studied. This is a low priority item, possibly with initial consideration by experts from CEN/ISSS WS/DIR before input into the PKIX WG.

The access to time-stamped certificates, CRLs and ARLs, need to be considered. These objects are not defined and thus cannot be retrieved from a Repository. This is a **low priority** item that could be considered by the PKIX WG from the IETF.

M. Protocol to interoperate with a Time Stamping Authority

The purpose of this work is to define a profile of the Time-stamping protocol under study by the PKIX working group, once this protocol will be published by the IETF. Also, ISO is in the early stages of producing a standard for time-stamping protocols and services (ISO/IEC WD 18014). It is first needed to support the work from the IETF, being the standard that is most likely to get market acceptance, (this is a **high priority** item) and then to establish this profile in a CEN/ISSS workshop (this is a **low priority** item).

N. Protocols for initial registration

The purpose of this work is to define additional registration protocols between users and Registration Authorities to allow registration without the need to exchange a secret by out-of-bands means. In addition registration protocols involving smart cards and in particular smart cards being able to generate the key pair themselves should be considered. This is a **low priority** item. This work could be done either by the PKIX working group, CEN (for smart cards) or by ISO.

O. APIs for infrastructure independence

The purpose of this work is to define APIs on top of the IETF operational and management protocols so that access to various PKI infrastructures can be made easier for implementers. The Open Group is traditionally defining APIs and could be considered to add this work item to its programme of work. This is a **medium priority** item.

P. Definition and support of generic roles

The purpose of this work is to define generic roles that could then be required to validly sign some contracts by people acting under a role in their organization or company. It is recommended that

the ICC define generic roles that are relevant to current transactions or contracts so that they can then be included in either Attribute Certificates or Public Key Certificates as extensions. This is a **medium priority** item.

Since Attributes Certificates are appropriate to support such roles, participation to the current work on that topic undertaken by the PKIX WG from the IETF should be encouraged.

Q. Repositories for signature policies and /or contract types

The purpose of this work is to establish a central repository of signature policies and/or of contract types. The ICC (International Chamber of Commerce) repository being set up under the E-terms initiative could be extended to achieve this goal. It is recommended that this work item is addressed as a **medium priority** item and to contact the ICC so that they can consider this opportunity.

8.3.4 Studies and pilots projects

R. Signature Policy

The concept of a signature policy has been identified as an important aspect for establishing a common basis for electronic signatures. ETSI TC/SEC has initiated work concerning the technical aspects of a signature policy, which should be supported as a **high priority** item. A study into the general implications of this concept should also be started as soon as possible with a **medium priority.**

S. Other Studies

The following topics require further study as a **medium priority.** This should be initiated by industry and supported by the European Commission.

- Identification and naming

  A specific study on solving name forms and name collisions both from a technical and legal point of view is needed. An extension to handle biometrics information in a certificate should also be specified. This topic is currently being partly addressed by the PKIX working group in the on going effort on "Qualified Certificate Profile" but might need to be complemented by either CEN or ETSI.

- Certificate path validation

  Studies are needed to handle name constraints and certificate policy constraints in the verification of a certification path. The current PKIX part 1 (RFC 2459) document does not fully address this concern and an extension to that document should be studied and then proposed to the PKIX working group.

- Role of notaries

  The purpose of this work is to identify the role of notaries in an electronic world both from a technical perspective and a business perspective and the requirements for CSPs supporting notarization services.

- Trusted Archival Services

  Archival services can play an important role in supporting electronic signatures that may need to be used in evidence long after they were created. As yet no standards exist for the use of such services in support of electronic signatures. This is an area requiring further study.

- Scalable revocations

  Studies are needed on the way to handle large numbers of revoked certificates.

- Scaleable suspensions

  Studies and explanations are needed on the way to handle suspended certificates in the context of their use in Electronic Signatures.

- Requirements for CSPs issuing Attribute Certificates

  The requirements for policy and security management standards for CSPs issuing Attribute Certificates need further study.

T. Interoperability Trials

It is important to get practical experience with the problems of interoperability, based on implementations of proposed standards from different suppliers. Trials should be performed in co-operation between suppliers and users. The IST Fifth Framework Programme and the ISIS Programme could be instrumental in supporting such trials.

Trials are particularly required in the following **high priority** area:

- Electronic signature syntax and encoding formats
- The use of X.509 certificates as qualified certificates
- Protocols to interoperate with a time-stamping authority

These trials need to incorporate the application of realistic signature and certificate policies so that the impact of policy issues on inter-working can be identified.

U. Pilots projects for APIs

There is a need for pilot projects regarding software portability, both for high level and low level APIs:

- High level APIs allowing generation and verification of electronic signatures using the Electronic Signature syntax and encoding format referenced previously.
- Low-level APIs interfacing a PKI and using the PKIX protocols.

It might be valuable to consider making the code developed for these APIs publicly available.

8.3.5 Conformity Assessment Activities

For all standards of the type ”Specification” above, and especially items B, C, D and F, there is a need for a harmonized and mutually accepted scheme for international conformity assessment. This has **high priority**, and the development of such a scheme should be entrusted to the European co-operation for Accreditation (EA).

V. Certification/registration of standards conformance of products and services for electronic signatures

The purpose of this work is to define requirements and guidelines for bodies that operate third-party certification/registration of conformance to standards in the following areas:

- Secure signature creation devices
- Trustworthy systems and products used by CSPs issuing qualified certificates
- CSP security management systems
- Certificate policies
- Signature creation and verification products
- Technical interoperability standards

It is recommended to undertake this work with a **urgent priority** within the European co-operation for Accreditation (EA), sectorial group for IT and Telecommunications Workshop with a target date of T0 + 3Q for the delivery of EA Guidelines. Later, this work should be extended to the co-operation within IAF (International Accreditation Forum). The resources needed have to be estimated together with EA.

8.4 Summary of work areas

The following table provides a summary of the high and medium priority work areas, as well as suggested responsible bodies and target dates.

Prio-rity	**Work area**	**Responsible Body**	**Target T0+**
Urgent	First set of components, fulfilling the framework for qualified electronic signatures (A)	Joint CEN-ETSI	2Q
Urgent	Specification of security requirements for trustworthy systems used by CSPs issuing qualified certificates (D)	CEN	2Q
Urgent	Specification of security requirements for hardware devices used as secure signature creation devices (F)	CEN	2Q
Urgent	Standard for the use of X.509 public key certificates as qualified certificates (I)	IETF and ETSI	2Q
Urgent	Certification/registration of conformance of products and services for electronic signatures (V)	EA	3Q
High	Security management and certificate policy for CSP issuing qualified certificates (C)	CEN	4Q
High	Specifications and guidelines for signature creation and verification products (G)	CEN	4Q
High	Electronic Signature syntax and encoding formats (H)	ETSI	2Q
High	Technical aspects of signature policies (R)	ETSI	2Q
High	Interoperability trials of proposed standards (T)	Users and industry	4Q
High	Protocol to interoperate with a Time Stamping Authority	IETF	2Q
Med	General CSP security management (B)	CEN	
Med	Security management and certificate Policy for CSP issuing Trusted Time-Stamps (E)	CEN	
Med	Standard for the profiling of CRLs, ARLs, OCSP responses and Time-Stamps (J)	ETSI	
Med	Use of smart cards for creation of electronic signatures and storage of other PKI objects (K)	ISO/IEC JTC1/SC17	
Med	APIs for infrastructure independence (O)	Open Group	
Med	Definition and support of generic roles (P)	ICC	
Med	Repositories for signature policies and/or contract types (Q)	ICC	
Med	General aspects of signature policy (R)	CEN	
Med	Further studies in several areas (S)	Industry	

Annex A. Inventory of Relevant Work

The sections for Germany, United Kingdom United States and Canada are excerpts taken from the report prepared by DOMUS for Industry Canada "Certification and Accreditation for PKIs" and "Certification Authorities" - Survey of Standards, Trends and Identification of Potential Models". Reference: http://www.domus.com/itss/papers.html

The sections for Italy, ICC, UNCITRAL and OECD are excerpts from the report "The legal aspects of digital signatures", prepared by the "Interdisciplinary Centre for Law and Information Technology" at K.U. Leuven for DGXV of the European Commission.

Reference: http://www.law.kuleuven.ac.be/icri/projects/projects_eng.htm

A very extensive compilation of national and international activities can also be found at:

http://www.law.kuleuven.ac.be/icri/projects/digisig_lb_eng.htm

A.1 International Standardization

An excellent summary of international standardization in this area was produced as part of the EU ETS project. It can be found at: http://www.quercus.co.uk/

A.1.1 IETF

The PKIX working group within IETF is currently very active, with a number of work items related to digital signatures and certificates. The following standards and drafts, relating to Internet X.509 PKI, have high relevance for EESSI:

- Certificate and CRL Profile (RFC 2459)
- Certificate Management Protocols (RFC 2510)
- Certificate Request Message Format (RFC 2511)
- Certificate Policy and Certification Practices Framework (RFC 2527)
- Operational Protocols - LDAPv2 (RFC 2559)
- LDAPv2 Schema (RFC 2587)
- Operational Protocols: FTP and HTTP (RFC 2585)
- Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API) (RFC 2479)
- Online Certificate Status Protocol – OCSP (RFC 2560)
- Certificate Management Message Formats
- Time-Stamp Protocols
- Qualified Certificate Profile
- Attribute Certificate Profile for Authorization

Reference: http://www.ietf.org/html.charters/pkix-charter.html

A.1.2 ISO/IEC JTC1/SC27

WG1 from SC 27 (Security techniques) has two projects which are particularly relevant to the topic.

- A technical draft report: ISO/IEC **PDTR 14516**: Guidelines on the use and management of TTP services.

This work started years ago. It provides an overview of the various kinds of TTPs with their main characteristics.

- A working draft: ISO/IEC **WD 15945**. Specification of TTP Services to support the Application of Digital Signatures.

This document duplicates some of the material of the previous document. Its content is still under discussion, in particular whether the document should be split into two parts. The first part would contain the description of the services and the definition of message names and message flow, the second one would contain the data structures of the messages in ASN.1 notation.

Other relevant SC27 standardisation activities are:

SC27 Document
ISO/IEC 9796: Digital signature schemes giving message recovery, ISO/IEC FCD 9796-1: 1998 (revision of ISO/IEC 9796: 1991)
ISO/IEC 9796-2: 1997, Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function
ISO/IEC WD 9796-3: 1996, Digital signatures schemes giving message recovery - Part 3: Mechanisms using a check function
ISO/IEC FCD 9796-4: 1998, Digital signature schemes giving message recovery - Part 4: Discrete logarithm based mechanisms
ISO/IEC 9798-3: 1998, Entity authentication - Part 3: Mechanisms using digital signature techniques (2nd edition)
ISO/IEC 9979:(1999), Procedures for the registration of cryptographic algorithms (2nd edition awaiting publication)
ISO/IEC CD 10118-1: 1998, Hash-functions - Part 1: General (2nd edition, revision of ISO/IEC 10118-1: 1994)
ISO/IEC CD 10118-2: 1998, Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm (2nd edition, revision of ISO/IEC 10118-2: 1994)
ISO/IEC 10118-3: 1998, Hash-functions - Part 3: Dedicated hash-Functions
ISO/IEC 10118-4: 1998, Hash-functions - Part 4: Hash-functions using modular arithmetic
ISO/IEC TR 13335-1: 1996, Guidelines for the management of IT Security (GMITS) - Part 1: Concepts and models for IT Security
ISO/IEC TR 13335-2: 1997, Guidelines for the management of IT Security (GMITS) - Part 2: Managing and planning IT Security
ISO/IEC TR 13335-3: 1998, Guidelines for the management of IT Security (GMITS) - Part 3: Techniques for the management of IT Security
ISO/IEC PDTR 13335-4: 1998, Guidelines for the management of IT Security (GMITS) - Part 4: Selection of safeguards
ISO/IEC PDTR 13335-5: 1998, Guidelines for the management of IT Security (GMITS) - Part 5: Safeguards for external connections
ISO/IEC 13888-1: 1997, Non-repudiation - Part 1: General
ISO/IEC 13888-2: 1998, Non-repudiation - Part 2: Using symmetric techniques
ISO/IEC 13888-3: 1997, Non-repudiation - Part 3: Using asymmetric techniques
ISO/IEC PDTR 14516: 1998, Guidelines on the use and management of Trusted Third Party

services
ISO/IEC FDIS 14888-1: 1998, Digital signatures with appendix - Part 1: General
ISO/IEC FDIS 14888-2: 1998, Digital signatures with appendix - Part 2: Identity-based mechanisms
ISO/IEC FDIS 14888-3: 1998, Digital signatures with appendix - Part 3: Certificate-based mechanisms
ISO/IEC WD 15292: 1998, Protection Profile registration procedures
ISO/IEC FDIS 15408-1: 1998, Evaluation criteria for IT Security - Part 1: Introduction and general model
ISO/IEC FDIS 15408-2: 1998, Evaluation criteria for IT Security - Part 2: Security functional requirements
ISO/IEC FDIS 15408-3: 1998, Evaluation criteria for IT Security - Part 3: Security assurance requirements
ISO/IEC WD 15443: 1998, A framework for IT Security assurance
ISO/IEC WD 15446: 1998, Guide on the production of Protection Profiles and Security Targets
ISO/IEC WD 15945: 1998, Specification of TTP services to support the application of digital signatures
ISO/IEC WD 15946-1: 1998, Cryptographic techniques based on elliptic curves Part 1: General
ISO/IEC CD 15946-2: 1998, Cryptographic techniques based on elliptic curves Part 2: Digital signatures
ISO/IEC WD 18014: Time stamping services and protocols

Reference: http://www.iso.ch/jtc1/sc27/

A.1.3 CEN/ISSS

In February 1998, CEN/ISSS held an initial Workshop in the area of Public Key Infrastructure. The workshop should develop and seek consensus on a set of workshop agreements, related to the use of PKI with a particular emphasis in achieving pan-European interoperability while also supporting more limited efforts in implementing the basic concepts. The following work items were defined:

- Registration of specific X.509 extensions
- Expression of policy in terms of trust information
- The specification of a smart card for PKI
- Using X.509 certificates with smart cards for the private keys
- Policy and a proposed Certificate Practice Statement for a PKI using smart cards
- Naming for European interoperability

Unfortunately, no work has so far been initiated in these areas.

CEN/TC 224 has together with ISO/TC 68/SC 6 conducted a project on "Card related secure commercial and financial transactions on open networks". Part 4 of the report contains requirements for further standardization.

CEN/ISSS has recently for ICTSB administered a project to study how consumer requirements may be taken into account by standards. The project is relevant for EESSI in so far as it covers Smart Cards, Internet and Electronic Commerce.

Recently, CEN/ISSS has launched the FINREAD Workshop, which will validate a set of technical specifications for a secure IC card reader for bankcard payments and remote banking services delivered over the Internet and open networks. Input into the FINREAD Workshop will be provided by the FINREAD Consortium, which is operating in the framework of the ISIS programme.

Reference: http://www.cenorm.be/isss/

A.1.4 ETSI

ETSI Technical Committee Security (TC SEC) is the focal point for security standardization within ETSI. TC Security develops and maintains a security standards policy which apply to all of ETSI's technical work, for application to the work of all ETSI Technical Bodies.

TC Security has established an ad-hoc working group on TTP services. The group has published a technical report on Electronic Signature Standardization, which contains a number of recommended areas for standardization.

The results of the study has identified the following major areas of standardization, harmonisation and policy development that need to be considered:

- Naming conventions and constraints,
- Format of public key certificates and CRLs,
- Format of Electronic Signature tokens,
- Selection of protocols to inter-operate with CSPs.
- Non repudiation policy,
- Security Policy Practice statements for CSPs,
- Use of smart cards for Electronic Signature

The study concludes that the following is a specific work item relevant to the work of ETSI, which can be dealt with in the short term:

Electronic Signature Standardization for electronic commerce in particular for business to business transactions, focusing on the application of signatures for purchasing requisition, contracts, and invoices. Areas to be covered include the first four topics from the list above.

The other items in the list above are either for further study and consideration or will be dealt with in other fora.

At the time of writing this document, the ad-hoc TTP working group from TC Security group is first concentrating on the format of Electronic Signature tokens, i.e. the description in ASN.1 notation of the data structure of an Electronic Signature and the description of the constituents of a signing policy.

TC Security is also active in the areas of lawful interception and Internet related security issues.

Reference: http://www.etsi.org/SEC/sec.htm

ETSI has also established a Security Algorithms Group of Experts (SAGE) which is creating cryptographic algorithms and protocols specific to fraud prevention and unauthorized access to public/private telecommunications networks and user data privacy (note that the access to and work in this group is restricted).

Reference: http://www.etsi.org/SAGE/sage.htm

ETSI Project on Pay Terminals and Systems (PTS) has produced specifications for the standardization of equipment and systems for use with Integrated Circuit (IC) card systems for wired payment telecommunications terminals. This work is performed in close collaboration with

CEN TC224. PTS is in a unique position to assist in the convergence of fixed and mobile networks.

Reference: http://www.etsi.org/PTS/pts.htm

A.1.5 ICTSB

The Information and Communications Technologies Standards Board was jointly set up by the three European standards bodies CEN, CENELEC and ETSI, with the participation of specification providers as full partners.

The ICT Standards Board listens to requirements for standards and specifications that are based on concrete market needs and expressed by any competent source. The Board then considers what standards or specifications need to be created, and how the task will be carried out. The Secretariat for the ICTSB is provided by ETSI.

The objectives of the ICT Standards Board are:

- Analysis and co-ordination of standards/specification requirements received from any competent source and based on concrete market needs;
- Translation of standards/specification requirements into coherent, approved programmes (projects) of standardization;
- Allocation of projects to the different production mechanisms of the participating organisations on a project management basis.

Reference: http://www.ict.etsi.org/

A.1.6 W3C

The World Wide Web consortium is usually abbreviated W3C. The W3C's Extensible Markup Language (XML) Recommendation specifies a standard syntax for **structuring Web documents**. The content of the document structure is arbitrary; anyone can create a XML data structure (be it a bibliographic format or cooking recipe) as long as it is well formed. Considerable work related to electronic signatures and XML has already been performed by W3C.

Digital Signatures have already been applied to PICS 1.1 labels (PICS is the W3C system for applying content ratings to Web information). In this case there are two DSig-specific extensions to standard PICS labels. These are called "resinfo" (used to create cryptographic links between the signature and the information to which the label giving the rating is attached) and "sigblock" (the signature itself).

The PICS Signed Labels (DSig) 1.0 Recommendation was issued in May 1998. This specification was approved on the second round of voting by the W3C membership after the inclusion of a mandatory set of hash algorithms and signature suites so as to ensure application interoperability.

The Signed Document Markup Language (SDML) was issued in June 1998 as a W3C Note. This was developed by the Financial Services Technology Consortium (FSTC) as part of the Electronic Check Project.

Recently, W3C has founded a joint Working Group with the IETF. The mission of this working group is to develop an XML compliant syntax used for representing the signature of Web resources and portions of protocol messages and procedures for computing and verifying such signatures. The first meeting of the proposed WG will occur at the IETF meeting in Oslo, July 11-16.

Reference: http://www.w3.org/DSig/

A.1.7 PKCS Publicly Available Specifications from RSA Laboratories

RSA Laboratories' Public-Key Standards (PKCS) are a set of informal inter-vendor specifications (called standards but more appropriately referred to a publicly available specifications as their publication is not under independent control) developed by RSA Laboratories with representatives of Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell and Sun. The standards cover RSA encryption, Diffie-Hellman key agreement, password-based encryption, extended-certificate syntax, cryptographic message syntax, private-key information syntax, and certification request syntax, as well as selected attributes.

The following specifications are especially relevant to EESSI:

PKCS #1: RSA Encryption Standard:

PKCS #7: Cryptographic Message Syntax Standard

PKCS #10: Certification Request Syntax Standard: ascii, ms-word, ps and ps.gz

PKCS #11: Cryptographic Token Interface Standard

PKCS #12: Personal Information Exchange Syntax Standard

PKCS #15: Cryptographic Token Information Format Standard

Several of the PKCS specifications have recently been published by IETF as «informational RFCs».

Reference: http://www.rsa.com/rsalabs/pubs/PKCS/

A.1.8 European co-operation for Accreditation

Until now, the branches of European national accreditation bodies have been handled separately by EAC (European Accreditation of Certification) and EAL (European co-operation for Accreditation of Laboratories) concerned with certification bodies or with laboratories.

These organisations have joined to form European Accreditation (EA) which now covers all European conformity assessment activities:

- testing and calibration
- inspection
- certification of management systems
- certification of products
- certification of personnel
- Environmental verification under the European Eco-Management and Audit Scheme (EMAS) regulation

The members of EA are the nationally recognised accreditation bodies of the member countries of the European Union and EFTA. Associate membership is open to nationally recognised accreditation bodies in countries in the European geographical area who can demonstrate that they operate an accreditation system compatible with EN45003 or ISO/IEC Guide 58.

Within EA, the sectorial group on IT&T is responsible for certification of management systems for information security. It has recently taken on the task of looking at certification of Certification Authorities.

Reference: http://www.european-accreditation.org./

A.2 European Projects

A.2.1 ETS Projects

In 1992, DG XIII of the Commission of the European Communities, in consultation with SOG-IS, started addressing the issues of Trusted Services through its initiative on Electronic Signatures (ES) and Trusted Third Party Services (TTPs).

In 1996, and in preparation for a Council Decision, which would allow a full-blown Action Programme in this area, it was decided to launch a limited, preparatory programme, subsequently called " The European Trusted Services-ETS Programme ". This programme turned out to be the only activity undertaken, as, eventually, the Commission Services decided not to proceed with the originally planned Council Decision. The ETS programme was characterised by short studies of duration of one year or less and limited resources (<?3 million). However, the broad framework of the large Action Programme was retained to provide an ambitious scope for these projects, although it was obvious that the existing time and funding constraints would not allow realisation of the demanding objectives.

Over the last three years, DG XIII has conducted a number of projects in the framework of » European Trust Services - ETS». The objective of ETS, as originally conceived and planned for the Council Decision which subsequently dropped, was the investigation and possible resolution of issues related to the creation of an appropriate enabling environment for the use and provision, by industry and commerce, of security services such as authentication, non-repudiation, confidentiality and time-stamping. These services may be offered by pan-European Trusted Third Party (TTP) Service infrastructures, as required by the market.

ETS has addressed the resolution of the issues and the measures necessary for the design, specification and market-driven implementation of a European Trusted Third Party Service infrastructure which will support the information security services needed to enable the European and Global Information Infrastructure.

The goal of ETS has been to tackle, to the greatest possible extent, both the technical, economical, legal and regulatory aspects that govern the use of cryptography for authentication, confidentiality and non-repudiation, and to resolve the dilemma posed by the increasing importance of encryption in our information society.

Reference: http://www.cordis.lu/infosec/src/ets.htm

A.2.2 Fifth Framework Programme

The Fifth Framework Research Programme contains a Key Action II – New methods of work and Electronic Commerce, which has identified a number of Action Lines. The following areas are prioritized for 1999:

- Identification and authentication
- Secure electronic financial transactions
- Digital object transfer

A future priority area is:

- Advanced technologies to strengthen trust and enable new business that require a high yet flexible level of protection of information, such as personal data, digital content and electronic cash.

Reference: http://www.cordis.lu/ist/home.html

A.2.3 ISIS

ISIS is an initiative of the European Commission. It reinforces standardisation activity in the domain of ICT (Information and Communication Technologies) through up to 50% co-funded projects which apply, validate or demonstrate standards. Projects are carried out by consortia of partners from 2 or more member states of the European Union, although they are open to wider co-operation. ISIS is an industry- and market-oriented programme, it is not an R&D initiative under the Framework Programme.

Special attention is paid to identifying user requirements for standards and/or acceptance of new draft standards, as well as contributing to interoperability and validation of critical interfaces necessary for the proper interworking of services and applications.

Preparations have started for an 1999-2000 ISIS Call for Proposals.

Reference: http://www.ispo.cec.be/isis/

A.2.4 Trust Infrastructure for Europe (TIE)

The business objective of the project is to provide an infrastructure to support Electronic Commerce in Europe by developing interoperable certification authorities that supply digital signature, time-stamping and key recovery services within a clearly defined legal framework. The technical objective is to stimulate the development of interoperable products and to deliver the required solutions by meeting business needs for assurance - Authentication, Integrity, Non-Repudiation and, as appropriate, Confidentiality.

A.2.5 Emeritus

EMERITUS is a multi-nation industry-led project which focuses on the way Trust Service Providers (TSPs) relate both to each other and to their clients. It is helping to define the infrastructure for trust-relationships which enable both internal and cross-border e-commerce. EMERITUS has the objective of creating national Trust Services Associations (TSAs) co-operating through a Global Trust Services Union (GTSU).

EMERITUS focuses on the confidence in an interchange taking place between the parties in an electronic exchange. The degree of confidence, or trust, that is required will depend upon a number of factors, the inherent value of the transaction, how well-established is the relationship between the parties, the degree of certainty that the other parties are who they claim to be, and the degree of confidence that the integrity of messages is preserved, i.e. that agreed words and values have not been altered. Much of this trust will be established through the use of cryptographic and related functions delivered by third parties, known as Trusted Service Providers (TSPs) because of the nature of the services they provide.

The EMERITUS vision sees TSPs competing aggressively in the market for subscription to their services but co-operating to the extent necessary to establish a single global Trust Services Infrastructure (TSI). A TSI is much more than a Public Key Infrastructure (PKI) because it includes not just technical elements but also the enveloping legal, business, liability and regulatory relationships. A TSI embraces a range of services wider than just public key certification. It also explicitly excludes PKIs that are internal to an organisation or a closed user group and have no external trust relationships.

EMERITUS is led by the Alliance for Electronic Business (AEB) and also involves EEMA - The European Forum for electronic business and Fundacion para el Estudio de la Seguridad de las Telecomunicaciones (Foundation for the Study of Telecommunications Security - FESTE). Importantly, a number of Business Review Groups are being established, consisting of users of Trust Services, Trust Service Providers, suppliers of related products and governmental and regulatory bodies. These groups participate actively in the progression of the project. They validate all project outputs before they are placed into the public domain. This process is designed to

enhance the quality and market acceptability of the project's outputs. EMERITUS benefits from partial funding from the TEN-Telecom programme, managed by the European Commission DGXIII.

Reference: http://www.gtsu.org/workshops or http://www.eema.org/emeritus

A.3 National Activities

A.3.1 Germany

Germany passed digital signature legislation in August 1997. The stated purpose of this act «is to **establish general conditions under which digital signatures are deemed secure** and forgeries of digital signatures or manipulation of signed data can be reliably ascertained». A major element of the legislation is a requirement for CA licensing:

«*The operation of a certification authority shall require a licence from the competent authority. … operator of a certification authority guarantees compliance with the legal provisions applicable to the operation of such an authority shall be deemed to possess the necessary reliability. The required specialized knowledge shall be deemed available when the persons engaged in the operation of the certification authority have the necessary knowledge, experience and skill. The other requirements pertaining to the operation of the certification authority shall be deemed met when the competent authority has been notified in a timely manner by means of a* ***security concept*** *of the measures ensuring compliance with the security requirements of this Act and the ordinance having the force of law … and their* ***implementation has been checked and confirmed by a body*** *recognized by the competent authority.* «

Section 12 of the German Digital Signature Ordinance states that the «*The security concept … shall include all security measures and, especially, an overview of the technical components used and a description of the procedures used in certification…*»

The «security concept» document referred to in the German legislation is roughly equivalent to a «certification practice statement (CPS)». The CPS defines the equipment, policies and procedures which the CA uses to satisfy the requirements specified in the certificate policies that are supported by it.

The German Digital Signature Ordinance provides regulation with respect to certificates to be used for «all electronic information and communication services which are designed for individual use … based on transmission by means of telecommunications». The purpose, content and scope of the German Digital Signature Ordinance is very similar to the purpose, content and scope of a Certificate Policy as defined in the ISO X.509 standard and as used in the IETF PKIX Part 4 «Certificate Policy and Certification Practice Framework.

The minimum requirements for «*Testing of technical components*» are stated in terms of satisfying ITSEC evaluation requirements. These minimum requirements and an initial assessment of which IETF PKIX Part policy elements these requirements may relate to, are as follows:

a. All technical components are to be evaluated at least to ITSEC E2. (It is concluded that this requirement would likely relate to the IETF PKIX part 4 framework high level policy element: *4.6-Technical Security Controls*);

b. Key generation, key storage and signature functions have to be evaluated against ITSEC E4. (It is concluded that these requirements would likely relate to a subset of the IETF PKIX Part 4 framework of policy elements: *4.6.1-Key Pair Generation and Installation,* and *4.6.2-Private Key Protection*);

c. Terminals for commercial services have to be evaluated against ITSEC E4 (This requirement does not directly relate to specific policy elements within the IETF PKIX Part 4 framework. The scope of the framework does not address «terminals» as such. However, terminal-level policy

requirements can be addressed in the IETF PKIX Part 4 framework in the PKI-relevant terms of «end-entities», »subscribers» and «relying parties»).

The German certificate policy (i.e., the ordinance) is not written in accordance with the IETF standard format, however the elements in the regulation can be mapped to policy elements in the IETF PKIX Part 4 framework. The German certificate policy, as defined in the Digital Signature Ordinance, is a single policy and the level of the security requirements indicate that it is a high assurance certificate policy. The German legislation and regulation do not acknowledge that there may be business requirements for lower level assurance policies (i.e. rudimentary, basic and medium levels) for digital signature certificates in the multiple security policy environment which is evolving for electronic commerce.

Section 15 of the legislation states that certificates issued by other countries «*shall be deemed equivalent to digital signatures under this Act insofar as they show the same level of security*». It can be concluded that only high assurance certificate policies of other policy domains would satisfy the German criteria for equivalence. There will likely be a large segment of electronic commerce for which rudimentary, basic and medium level digital signature certificate policies will have no equivalencies in the German policy domain.

To support licensing of CAs, Section 15 of the regulations requires «*Checks on the certification authorities*». This requirement for CA accreditation or compliance audits is described as follows:

«*Before beginning its operation, following security-relevant changes and at regular two-year intervals the certification authority shall arrange for checks … and shall submit to the competent authority a relevant check report and confirmation showing that it fulfils the provisions of the Digital Signature Act and this Ordinance*»

It is presumed that this compliance audit would confirm that:

a. The CA has effectively implemented and is using the practices documented in its «security concept» (equivalent to a «Certification Practices Statement»); and

b. The «security concept» (equivalent to a «Certification Practice Statement») adequately addresses the requirements of the Digital Signature Ordinance (equivalent to a «Certificate Policy»).

A large effort has recently been launched in Germany to define **interoperability standards**. Several interoperability specifications have been published for certificates, time-stamps, signature formats and directory services; unfortunately all of them only in the German language. A German DIN standard for smart cards used as signature creation devices has recently been published in English.

Reference: http://www.bsi.de/aufgaben/projekte/pbdigsig/index.htm

Reference: http://www.regtp.de/Fachinfo/Digitalsign/neu/index.htm

A.3.2 Italy

Italy is the only Member State of the European Union where an adaptation of the law has recently been undertaken to authorize the use of electronic documents and electronic signatures for all kinds of purposes.

The Bassanini law

The law nr.59 of 15 March 1997 (the so-called Bassanini law) allows the use of electronic documents for legal transactions, the decree nr.513 of 10 November 1997 sets the criteria and methods to be used, and the draft decree on the technical rules lays down the specific technical requirements for electronic documents.

According to this law, full legal effect will be given to electronic documents and data of public administrations *and of private individuals* and to the electronic archiving and transmission of these documents and data.

The law further states that "the criteria and methods of application of this paragraph shall be set out, for the public service and for private individuals, in specific regulations.

Decree on Criteria and Methods

At its meeting on 5 August 1997, the Italian Council of Ministers approved a draft decree of the President of the Republic setting out "*Regulation on the criteria and methods of application of Article 15 (2) of Law 59 of 15 March 1997 on the formation, archiving and transmission of documents by computer and telematic methods*". It was definitively approved by the Council of Ministers on 31 October 1997.

Art. 2 of the decree provides that "computer documents by whomsoever they are drawn up, their storage on a data-processing medium and their transmission by telematic methods shall be valid and effective for all legal purposes if they abide by the terms of this regulation". According to art. 3, "the technical rules for the formation, transmission, storage, duplication, reproduction and validation, including time validation, of computer documents shall be laid down by Decree of the President of the Council of Ministers". A computer document is defined in art. 1 (1) a) as "the representation in electronic form of legally relevant acts, facts or data".

Art 4 (1) provides that "the electronic document fulfilling the requirements stated by this regulation shall satisfy the statutory requirement of written form". According to Art. 5 "a computer document signed by a digital signature in the sense of Art. 10 has the same evidentiary value as a private instrument - scrittura privata - in the sense of Article 2702 of the Civil Code".

The regulation is however not complete and effective since it requires the technical rules to be adopted (art. 3). It also requires technical rules concerning public services (art. 18, 3) and tax regulation (art. 4, 2).

Provisions on digital signatures

A "digital signature" is defined in Art. 1 (1) b) as "the result of the computerised validation procedure based on a system of paired asymmetric keys, one public and one private, allowing the signatory, by means of the private key, and the recipient by means of the public key, to demonstrate and verify the origin and integrity of a computer document or of a set of computer documents". Unlike the German Signaturgesetz there is no limitation to natural persons. The concept of the digital signature is defined in a purely technical matter. According to the Italian decree a digital signature can be the equivalent of a hand-written signature but it can also replace, for any purpose set out in the legislation, the affixing of seals, embossing, stamps, signs and marks of any kind.

Another interesting item in the Italian decree, and absent in the German Signaturgesetz - is the "authentication" of a digital signature by a notary of another public official. According to Art. 16 of the decree the authentication of a digital signature consists in the attestation by the public official that the digital signature has been attached in his presence by its owner, following establishment of his personal identity, the validity of the public key and the fact that the signed document reflects the will of the party and is not contrary to the legal order (…)"

Very important, from a European perspective, is Art. 8 (1) of the decree. It provides that "anyone intending to use a system of asymmetric encryption keys for the purposes set out in Article 2 must obtain an appropriate pair of keys and make one of these keys public by means of the certification procedure carried out by a certifying authority".

Consequently a digital signature will not be legally valid unless the public key has been certified by a certifying authority and this certifying authority has to receive an official accreditation prior to the commencement of its activities.

The certification authorities must be registered in an official public list kept by the AIPA - *Autorità per l'Informatica nella Pubblica Amministrazione* - and must possess the four requirements listed in Art. 8 (3): a) if the certification authority is a private person, it has to be a public limited company with a share capital of no less than the share capital necessary to receive

the authorisation to operate a bank activity, b) their legal representatives and managerial staff must possess the requirements of trustworthiness incumbent upon persons responsible for the management, direction and auditing of banks, c) the technical staff and the personnel employed on certification work, must fulfil certain conditions regarding competence and experience, and d) the computer procedures and related products must be of a quality that is in keeping with internationally recognized standards.

According to Art. 8 (4) the certification procedures may also be carried out "by a certifying authority operating under a license or authorization issued by another Member State of the European Union or the European Economic Area on the basis of equivalent requirements".

Draft decree on technical rules

At the end of August 1998 the AIPA approved a first draft on technical rules for the formation, transmission, storage, duplication, reproduction and validation, including time-validation of electronic documents. The draft is published for comments and observations and will afterwards be submitted to the president of the Council of Ministers for approval.

The draft decree lays down specific rules concerning

- the algorithms: the signature creation and verification algorithms and the hash algorithms (Art. I.2 and I.3),
- the key characteristics: the draft defines three kinds of keys: signature keys, certification keys and time-stamp keys (Art. I.4), and the minimum length of the keys: 1024 bit (Art.I.4)
- the key generation modalities (Art.I.5-7) and the key storage modalities (Art.I.8)
- the signature generation and verification (Art.I.9)
- the contents and form of the certificates (Art. I.11-12)
- the procedure for candidate CA's to request a license (Art. II.3-7), and the registration procedure for requesting a certificate (Art.II.8-9)
- the possibility of using pseudonyms (Art.II.10)
- the certificate generation, revocation and suspension procedures (Art. II.15-31)
- the CA requirements: security measures, personnel, quality system (Art. II.28-29 and II.32-38)
- the time-stamp modalities (Art. III.1-III.11)
- the storage modalities of electronic documents (Art. IV.1-2)
- the possibility for public administrations to act as a CA (Art.V.1-3)

Interesting is that a possible limitation of CA's liability has been introduced: the CA may provide a definition of obligations and a limitation of liability and damage compensation (Art. II.32). The draft decree also expresses the obligation to be licensed in order to deliver certification services (Art.II.3). The decree also states that if the legal effects of an electronic document last longer than the signature key, a time-stamp procedure has to be used (Art.IV.1). Related to the storage modalities the draft decree refers to an act of AIPA of 30 July 1998.

Conclusion

Italy is the only European Union Member State where digital signatures are legally equivalent to hand-written signatures. The equivalency depends however on very specific conditions. Only digital signatures in the strict sense of signatures generated by using asymmetric cryptography and with a signature key certified by an officially authorized certification authority are legally valid. Certification procedures may also be carried out "by a certifying authority operating under a license or authorization issued by another Member State of the European Union or the European Economic Area on the basis of equivalent requirements".

Reference: http://www.aipa.it/english/law[3/index.asp

A.3.3 United Kingdom

The UK Department of Trade and Industry (DTI) issued the Secure Electronic Commerce Statement in April 1998. This statement addressed potential changes to the legal and regulatory framework for electronic commerce in the UK. The UK intends to introduce legislation for the voluntary licensing of Certification Authorities.

«*…intend to introduce legislation to license those bodies facilitating the provision of cryptography services. … Certification Authorities. …Such licensing will be voluntary, as business has requested, although we hope that organizations providing services to the public will see the benefit of adhering to a high standard, and the public confidence that this will bring. We intend that licensed Certification Authorities –* ***conforming to the procedural and technical standards*** *which licensing will confer – would be in a position to support electronic signatures* ***reliable*** *enough to be recognized as equivalent to written signatures*»

It can be concluded from the above statement that the focus for UK licensing is for open community CA «*organizations providing services to the public*». The CAs operating within closed enterprise business environments may also voluntarily participate in the licensing scheme but these closed community CAs are of secondary interest.

The UK DTI statement refers to CAs conforming to «procedural and technical standards» as a condition for licensing. However, the UK DTI statement does not provide details regarding the intended criteria or if there is an envisaged Accreditation Scheme to assess reliability and the CAs' compliance with these standards. In addition, it does not explicitly identify the need for a «competent authority», as the German legislation has.

In the context of ensuring that there is security and trust for electronic commerce applications, the UK DTI statement does address the provision of accreditation for Business and Enterprise security:

«*The DTI, … is thus introducing an Accreditation Scheme to assess Businesses' compliance to BS 7799, the national standard on information security. The scheme being launched … will allow businesses the opportunity to have their implementation of information security professionally certified: giving their trading partners and customers greater confidence and trust. The Department is also chairing an industry working group to review and update the Standard with the aim of making it a global benchmark …* »

A.3.4 Belgium

Legal situation

On the 12th June 1998, the Belgian Council of Ministers has approved a law proposal related to the activity of the agreed CAs. This Law determines the general conditions for the Certification Authorities to be recognised and the legal regime applicable to their activities and the rules to be taken into account as well by CAs as by end-users, in order to assure the security of, and the trust in the use of the digital signature. One of these conditions being those to ensure the interoperability of the certification systems. The accreditation is on a voluntary basis and the end-user is free to use an accredited CA or not in the context of digital signature. The procedure to collect information in order to verify the identity of the subjected entity should be in line with the rules and law for the protection of private life.

The law proposal provides under which conditions a certificate of a European Member State or another country can be accepted as equivalent to a certificate issued by an accredited CA. The administration should keep a list of certificates, which could be accepted as equivalent to the ones issued by a recognised CA.

On the 26th of March 1999, this law proposal was approved at the second reading, after the advice of the Council of State.

The AGORA project

AGORA is a project launched by the Belgian Federal Government. The first phase of the project has lead to the set-up of an Memorandum of Understanding (MOU) aiming the interoperability of the digital signature systems in Belgium. The idea is to serve the interests of the Administrations having to cope with several existing systems when they exchange signed documents either with other administrations or with external entities.

The second phase is based on a partnership consisting of the following organisms: Ministry of Finances, Banque Carrefour and National office of the Social Security, Ministry of Economic affairs, National Register and the current active security service providers i.e.: Belsign, Belgacom, Isabel and Publilink. The objective of the second phase is to develop a pilot project implementing the interoperability between the services offered by the providers, partners of the project. This interoperability will allow the client of a service to verify the signature of his partner even if this partner is affiliated to another service.

The AGORA project – Phase I (mid 1997 – end 1998)

This phase resulted in a document called 'Protocole d'Accord' (MOU), after 18 months of study and discussions. This agreement was the expression of a consensus on how to reach compatibility and interoperability of electronic signature components. The interoperability target was driven in the interest of the user, and more particularly to cover the requirements of Belgian Administrations in their communication between them and with the citizens.

The partners which have collaborated to this 'Protocole d'accord' were as well representatives from the administrations as representatives from the industrial sector:

During the last two months of the Phase I, three documents were published, that represent a significant reference for the objectives of AGORA Phase II. These documents are:

- Proposal for Belgian Law, related to the activities of Certification Authorities accredited for the use of signatures, and presented to the Council of Ministers on 12 June 1998;
- "Proposal for a European Parliament and Council Directive on a common framework for electronic signatures" (EUROPEAN COMMISSION COM(1998) 297 final 13.05.98)" ;
- 'Protocole d'Accord' on security techniques, published by EEMA (European Electronic Messaging Association).

The AGORA project – Phase II (begin 1999 – March 2000)

The objective of AGORA Phase II consists of:

- In the first place, to allow a user to subscribe to one service only, in order to verify every signature, independently of the service provider to which the signer has subscribed (interoperability level 1).
- In a second place, to make it possible for the user to develop and implement software that integrates signature creation and verification operations, and this independently of the service providers (interoperability level 2).

A.3.5 Sweden

In Sweden, the non-profit organization SEIS has developed a number of national technical and administrative standards for the production, distribution and use of Electronic ID-cards, i.e. smart cards containing private keys and certificates. The EID cards can be used for authentication, encryption and electronic signatures. The smart card standard has served as the basis for the development of the PKCS#15 specifications from RSA Laboratories. The certificate profile has served as input for the IETF PKIX draft for Qualified Certificates.

SEIS has also developed S10, a proposed certificate policy for «High assurance general ID-certificate with private key protected in an electronic ID-card». The policy is currently being adopted by the Swedish Banker's Association.

The Swedish standards are presently used for EID cards both in the private sector and government.

Reference: http://www.seis.se

A.3.6 Spain

In Spain, there is not any approved regulation about electronic signature. But, it is allowed to use encryption in computer communications based on the "General telecommunications law" (11/1998 of 24th of April, art. 52, 1 and 2).

In the Public Administration there are general rules that allow the use of security measures, to seal electronic data transfer (RD 263/1996 of 16th of February). There are also partial regulations referred to Taxes declarations (O. of 22nd of March 1996), and to Spanish Healthcare Institut (Resolution of 17th of January of 1996), using EDI or secure electronic communication.

Several Spanish ministries are preparing the regulation of the electronic signature European Directive in the Spanish market.

There are several initiatives aimed to trigger the telecommunication security infrastructure:

- The Spanish MINT has been allowed to create a PKI (government budget law of 1998, art. 81 of law 66 of 30th of September of 1997).
- The Spanish MINT and UPC have set up a Time Stamping Protocol specification and implementation, within the ETS II project PKITS. This protocol includes a linking mechanism to make more difficult to "include" out of band (fake) Time Stamps .
- An important experience, is the Personal Tax Declaration submission through Internet, using advanced electronic signatures (Order of 13th of April of 1999).
- The project AEQUITAS-PROCURADORES has developed a software tool integrated in the Spanish Court management application: LIBRA. The application allows the transmission of court notifications and other documents from court to court, and between the court and the Procurers, using advanced electronic signatures.
- There is a Spanish Association of TTP services providers created by the Spanish MINT, FESTE and ACE (all of them CSP in Spain). This association has been promoted by the EMERITUS project, that wants to establish such a kind of associations all over the world. The members of these associations will accept the telecommunications security policies established by the governments.
- There are also plans to establish a voluntary accreditation schema for Certification Service Providers by FESTE (Foundation for the Study of Telecommunications Security). This foundation was created by the Spanish associations of notaries, commerce agents, and lawyers, as well as University of Zaragoza and Intercomputer S.A.

A.3.7 United States of America

There are a number of proposed US **federal** legislative initiatives, which address aspects of CA accreditation. While there is no certainty that any of these proposals will be passed into law, they do provide some insight as to the direction in which the US may be headed with respect to potential accreditation of CAs. Three legislative initiatives of interest are:

a. *Electronic Financial Services Efficiency Act* of 1997;

b. *Digital Signature and Electronic Authentication Law* of 1998 - Technical Amendments to the *Bank Protection Act* of 1968; and

c. *Electronic Commerce Enhancement Act* of 1997.

The stated purpose of the *Electronic Financial Services Efficiency Act* is to «*define and harmonize the practices, customs, and uses applicable to the conduct of electronic*

authentication.» This Act makes no distinction between open community CAs and closed community CAs. Some major elements of the Act are:

a. To establish a National Association of Certification Authorities;

b. To require all CAs, providing electronic authorization services in the US, to be members of the Association;

c. To require the Association to establish an Electronic Authentication Standards Review Committee;

d. To require the Association's Standards Review Committee to establish and adopt guidelines, standards, codes of conduct used by members of the Association. These criteria would include rights and responsibilities of CAs matters involving: notification; disclosure; liability of consumers and CAs; and disciplinary procedures; and

e. To require the US Secretary of the Treasury to provide effective oversight of the Association's Standards Review Committee

The stated purposes of the amendment to the *Bank Protection Act* are to:

a. «facilitate the participation by financial institutions in the burgeoning area of electronic commerce»;

b. «provide that the interests of consumers are adequately protected»; and

c. «avoid the effects of premature or conflicting regulation that could inadvertently impede the development of electronic banking and commerce or imperil the security of electronic banking and commerce.»

The stated purpose of the *Electronic Commerce Enhancement Act* is to enhance electronic commerce by requiring US federal «*agencies to use digital signatures, which are compatible with standards for such technology used in commerce and industry*». The Act recognizes that US government agencies may operate a closed community CA or may use the services of an open community CA. A major element of the Act is to require the Director of the Office of Management and Budget to issue guidelines which would include requiring agencies to accept certificates issued by:

a. the agency's CA; or

b. a CA which is «*licensed or accredited by a State or local government or an appropriate accreditation body*».

Notwithstanding there not being US federal enabling legislation, there is some movement towards regulation of CAs by individual federal regulatory authorities using their existing terms of reference.

The US federal government's position with respect to accreditation of CAs is evolving. However from the insight provided from the White House-issued «A Framework for Global Electronic Commerce» and the legislation being discussed and debated in Congress, it can be concluded that there may be movement towards:

a. Supporting voluntary CA accreditation;

b. Recognizing that any statutory regulations regarding CA accreditation should not replace contracts, prior relationships and other controls as implemented between parties to the transactions in closed community CA communities such as in the financial services industry. Most such closed systems operate across open networks with business interests and trading partners located in many US states and international jurisdictions;

c. Providing legal recognition to authentication mechanisms where the parties to a transaction have determined appropriate technical and procedural methods of authentication, by contract or prior agreement; and

d. Recognizing that contracts should be enforced to facilitate effective global electronic commerce in closed systems, without undue regard to statutory regulations, which may be more applicable to the open community CAs.

Government and industry representatives from the US and other nations, including Canada, participated in the April 1998 Copenhagen Hearing. At this hearing, many of the views expressed by US participants supported voluntary CA accreditation and accommodating the contractual business model of closed community CAs. In particular, concern was raised regarding how new government liability rules for CAs, such as those passed by Germany or those being considered for EU Directive, should not have negative impact on existing closed systems.

At the **state** level, some 43 states have enacted legislation to regulate electronic authentication. In adopting such laws, states have generally followed one of three approaches:

- A comprehensive approach, with specific conditions for digital signature techniques (6 states, most importantly Utah, Washington, Minnesota)
- Minimalist approach (14 states)
- Sectorial approach (23 states)

The states specifying digital signature techniques have also specified that the NIST CS-2 Protection Profile Guidance shall be used for accreditation/licensing evaluation.

A.3.8 Canada

The Government of Canada Public Key Infrastructure, which is a closed community PKI, is using a layered approach to achieving accreditation:

a. FIPS PUB 140-1 Validation of Cryptographic modules;

b. CSE Endorsement of CA Products;

c. Security Certification of PKI Architectural Components; and

d. Accreditation of PKI CA Domains.

FIPS PUB 140-1 Validation of Cryptographic modules – This process identifies the standard security level for protection of sensitive information to be satisfied by a cryptographic module utilized within a security system (i.e. end-entity clients, CAs and LRAs).

CSE Endorsement of CA Products – Endorsement signifies that the security policy of a product meets minimum standards confirmed through rigorous analysis and testing by the Canadian Communications Security Establishment (CSE) in accordance with the Cryptographic Endorsement and Assessment Program (CEAP).

Security Certification of PKI Architectural Components – Security «certification» is defined as «*the comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation, that establishes the extent to which a system satisfies a specified security policy*».

Accreditation of PKI CA Domains – The Government of Canada security policy considers each department to be an individual enterprise, which is responsible for development and management of their own security policies, in the context of conducting threat risk assessments to identify and accept residual risk. Thus, in the case of the GOC PKI, the accreditation authority responsibilities are distributed among the stakeholders:

a. The Communications Security Establishment is responsible for accreditation of the root CA for GOC PKI supported Certificate Policies; and

b. Individual departments are responsible for accreditation of their individual CA domains for supported Certificate Policies.

In the context of the GOC PKI, the term «accreditation authority» is roughly equivalent to the «competent authority» as used in the German digital signature legislation.

To maintain the accreditation decisions, there is a key ongoing role for the Certification Practice Statements to document the operational practices of CA domains for particular Certificate Policies which may require particular safeguards. The GOC PKI Policy Management Authority (PMA) approves all Certification Practice Statements and Certificate Policies for use across the GOC PKI.

A.4 Other International Activities

A.4.1 International Chamber of Commerce (ICC)

GUIDEC

The GUIDEC - General Usage for International Digitally Ensured Commerce - has been developed in 1997 by the ICC in order to provide a set of common definitions and business-generated best practices for certifying and "ensuring" electronic commerce. The GUIDEC therefore adopts the specific term, "ensure", to describe what elsewhere is called a "digital signature" or "authentication", in an attempt to remove the element of ambiguity inherent to other terms employed.

The GUIDEC treats the core concepts, best practices and certification issues in the context of international commercial law and practice. In so doing, the document assumes practices in which transacting parties are expert commercial actors - so-called business-to-business - , operating under the lex mercatoria.

Although the GUIDEC is organised primarily as an outline for parties involved in public key based systems (i.e., "digital signatures"), the fact that it draws upon existing law means that it is not technology specific; it may be equally applied to paper-based and other methods.

The GUIDEC is strongly inspired by the Digital Signature Guidelines of the Information Security Committee of the Science and Technology Division of the American Bar Association, and attempts to enhance some of the concepts set out therein from an international and commercial point of view. The document also draws upon and extends existing international law treatment of digital signatures in particular that articulated in the United Nations Model Law on Electronic Commerce (UNCITRAL Model Law).

E-terms

The E-terms service will be based on an on-line repository containing all the tools that are necessary to compose contracts on-line and conduct electronic transactions with a minimum of legal risk. Rules and terms of different kinds that might apply in the digital environment can be incorporated into electronic contracts by referring to a unique identifier automatically supplied by the E-terms repository. A prototype of the repository and service will go "live" for one year in 1999 for tests among a group of volunteer users. E-terms will be especially useful for small and medium sized enterprises that do not have their own in-house legal expertise.

Reference:
http://www.iccwbo.org/Commissions/Commercial_practice/Electronic_commerce_project.htm

A.4.2 OECD

The OECD is since a few years heavily involved in promoting a, both technically and legally, secure framework for electronic commerce. Diverse reports, recommendations and conferences envisage the issues invoked by the electronic transmission of information for different purposes.

An important document of the OECD relevant for the regulation of digital signatures is the set of "Guidelines for Cryptography Policy". These Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that they will be widely read and followed by both the private and public sectors.

With regard to electronic commerce in general the OECD organised in November 1997 an international conference in Turku, Finland. The discussion document for this conference, with the title "Dismantling the barriers to global electronic commerce".

With regard to digital signatures and certification policies an important OECD-document is the 1997 report on Certification in the Electronic Environment and the 1997 paper "Public Policy and Technology Architecture Options for Certifying Information on Global Networks". These documents are essentially limited to an overview of the technological directions in the development of certification mechanisms and independent trusted services, and of the key policy issues regarding the legal treatment of digital signatures and certification authorities.

The latest OECD initiative was the "Joint OECD-Private sector workshop on Electronic Authentication" in Palo Alto, June 2-4 1998. The conference built on the ministerial-level conference on electronic commerce in Ottawa, October 1998.

Reference: http://www.oecd.org/dsti/sti/it/

A.4.3 UNCITRAL

Model Law

The United Nations Commission on International Trade Law (UNCITRAL) in 1996 adopted its Model Law on Electronic Commerce. This Model Law aims to harmonise and unify the law of international trade in an electronic environment. Member States are invited to make use of the Model Law when developing or enhancing national legislation. A Guide to Enactment, accompanying the Model Law, provides for background and explanatory information.

The Model Law proposes a set of internationally acceptable rules related to the introduction of paperless transactions having legal significance. It was, indeed, noted that the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity.

Typical issues, such as the national requirements of "writing", "signature" and "original", are addressed by the Model Law and consideration is given to extend the scope of such notions to an electronic environment. In order to provide for a legal extension the Model Law relies on the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirements with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. It should be noted, however, that the functional-equivalent approach has been taken with respect to the concepts of "writing", "signature" and "original" (Articles 6-8) but not with respect to other legal concepts dealt with in the Model Law. For example, article 10 does not attempt to create a functional equivalent of existing storage requirements.

Draft Uniform Rules on Digital Signatures

For the thirty-second session of the Working Group on Electronic Commerce in Vienna on 19-30 January 1998, the Secretariat of the Working Group prepared a note "*Draft Uniform Rules on Electronic Signatures*". This note contains revised draft provisions to be considered for possible inclusion in the Uniform Rules. They were prepared pursuant to the deliberations and decisions of the Working Group at its thirty-first session, as reflected in the Report of that session. In particular the draft provisions are based on the working assumption of the Working Group that its work in the area of digital signatures would take the form of draft statutory provisions, and that possible uniform rules in this area should be derived from article 7 of the UNCITRAL Model Law on Electronic Commerce.

Contents of the Draft Uniform Rules

Although it is currently too early to investigate the impact of the work of the UNCITRAL some basic conclusions can already be derived from the preliminary draft texts of the Working Group on Electronic Commerce.

The Draft Uniform Rules include provisions on digital signatures, other electronic signatures, certification authorities and related legal issues.

The latest version of the Rules makes, like the draft Illinois Electronic Commerce Act, a distinction between the concepts of “electronic signature” and “secure electronic signature”. A “secure electronic signature” can be a “digital signature” but it can also be another kind of electronic signature provided that it meets certain standards. A data message authenticated by means of a secure electronic signature is presumed not to have been altered and to bear the signature of the person to whom it relates but this presumption can be rebutted, for instance by evidence indicating that the security procedures were not implemented correctly (current article 3).

Related to certification authorities the draft rules define “Certification authority" as any person who, or entity which, in the course of its business, engages in issuing [identity] certificates in relation to cryptographic keys used for the purposes of digital signatures.

A certificate is defined as follows:"[Identity] certificate" means a data message or other record which is issued by a certification authority and which purports to confirm the identity [or other significant characteristic] of a person or entity who holds a particular key pair.

Interesting is that the provisional article 8 of the Rules states that such a certificate shall, as a minimum:

(a) identify the certification authority issuing it;

(b) name or identify the [signer][subject of the certificate] or a device or electronic agent under the control of [the signer][the subject of the certificate][that person];

(c) contain a public key which corresponds to a private key under the control of the [signer][subject of the certificate];

(d) specify the operational period of the certificate;

(e) be digitally signed or otherwise secured by the certification authority issuing it;

[(f) specify the restrictions, if any, on the scope of use of the public key;] [and]

[(g) identify the algorithm to be applied].

A.4.4 American Bar Association

The Information Security Committee of the Electronic Commerce Division of the American Bar Association has been the focal point of diverse electronic commerce law initiatives since the Division's formation in 1992. The Committee explores current computer security issues including those related to public key infrastructure, cryptology, risk analysis, standards, "commercial responsibleness" and the legal efficacy of secure digital commerce.

The most well-known result of ABA-ISC in this area is the document «Digital Signature Guidelines», which was published in 1996. The Guidelines are significant in that they are the first (and pre-eminent) statement of legal principles for certificate-based use of digital signatures. They are particularly important in the US in the absence of specific law on the subject.

The ISC is presently working on a set of «PKI Assessment Guidelines» (PAG), which are intended to be used to assure a trustworthy PKI by developing certificate polices and accreditation guidelines for evaluators of Certification Authorities and other PKI components.

Reference: http://www.abanet.org/scitech/ec/isc/home.html

A.5 Security Evaluation Criteria

Criteria are the "standards" against which security evaluation is carried out. They define several degrees of rigour for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product (or system) to meet each Assurance level.

A.5.1 TCSEC

The US Department of Defense published the first criteria in 1983 as the Trusted Computer Security Evaluation Criteria (TCSEC), more popularly known as the "Orange Book". The current issue is dated 1985. The US Federal Criteria were drafted in the early 1990s as a possible replacement but were never formally adopted.

A.5.2 ITSEC

During the 1980s, the United Kingdom, Germany, France and the Netherlands produced versions of their own national criteria. These were harmonised and published as the Information Technology Security Evaluation Criteria (ITSEC). The current issue, Version 1.2, was published by the European Commission in June 1991. In September 1993, it was followed by the IT Security Evaluation Manual (ITSEM) which specifies the methodology to be followed when carrying out ITSEC evaluations.

A.5.3 Common Criteria

The Common Criteria project was initiated to harmonise the ITSEC, CTCPEC (Canadian criteria) and US Federal Criteria (FC) into a Common Criteria for Information Technology Security Evaluation (CC) for use in evaluating products and systems and for stating security requirements in a standardised way. Its aim is to replace national and regional criteria with a world-wide set acceptable to the International Standards Organisation.

Government agencies from Canada, France, Germany, the Netherlands, the United Kingdom and the United States sponsor the project. Version 1.0 was published on 31st January 1996 and following trials and comments, Version 2.0 (final draft) was published in December 1997. Common Criteria Version 2.0 will be submitted to ISO for formal acceptance as an international standard in 1998.

The Common Criteria Implementation Board (CCIB) has been established to act as the technical liaison and information transfer point for users of the CC.

The Common Criteria is issued as an International Standard ISO/IEC 15408.

Common Criteria – Protection Profiles

Within the Common Criteria scheme "Protection Profiles" are specified which identify a set of functional and assurances requirements for IT systems performing a specific function (e.g. general purpose IT systems, firewall). Two protection profiles are of particular relevance to EESSI:

- **CS2:** The purpose of CS2 is to provide the guidance necessary to develop "compliant" protection profiles for near-term achievable, security baselines using commercial off the shelf (COTS) information technology. This profile has been defined by NIST in America.
- **Smart Card Protection Profile:** Several protection profiles are known to exist for smart cards, including two registered with the French Certification Body under the numbers PP/9806, produced by a consortium of 6 companies, and PPnc/9809,. produced by "Eurosmart", the European smart card association

A.5.4 BS 7799

The British Standard BS 7799 is intended for use as a reference document by managers and employees who are responsible for initiating, implementing and maintaining information security

within their organization. It is identifies commonly accepted policy and best practices for the security of information. It brings together requirements / guidance on procedural and technical controls.

BS 7799 can either used as guidance or is the basis for accreditation of an organisations security. This is reflected in the two parts as follows:

1. BS 7799: Part 1:1995 is *The Code of Practice* - provides guidance material to help companies to implement their own information security system; This British Standard provides a comprehensive set of security controls comprising the best information security practices in current use, both in the UK and internationally

2. BS 7799: Part 2:1998 is *The Requirements Specification* - against which an organization is assessed for compliance and subsequent certification. This part of BS 7799 specifies requirements for establishing, implementing and documenting information security management systems (ISMS). It specifies requirements for security controls to be implemented according to the needs of individual organizations.

Part 2 specifies mandatory requirements for accredited use of the controls described by guidance in part 1.

BS 7799 part 1 and the detailed controls in part 2 have been updated and are due to be published in April 99. A number of associated guidance documents exist.

BS 7799 accreditation is a requirement of providers of service providers under upcoming UK Electronic Commerce legislation.

BS 7799 is being used in a number of European and other nations including: Norway, Sweden, Brazil, Denmark, Australia, New Zealand, Japan. This includes use for accreditation of CSPs.

BSI have set up the organization «c-cure» to promote the BS 7799 based accreditation systems. A number of companies offer services to BS 7799 accredit organizations.

Reference: **http://www.c-cure.org/**

A.5.5 FIPS 140-1

Issued in 1994 by NIST (US National Institute of Standards), FIPS 140-1 specifies the overall requirements for the design and implementation of modules that use cryptographic algorithms and methods. The standard identifies requirements for four security levels for cryptographic modules to provide for different sensitivity levels of data from low value to high value, and for many different applications.

NIST has established a program to validate cryptographic modules for correct implementation of cryptography standards. This effort is carried out under the auspices of the National Voluntary Laboratory Accreditation Program (NVLAP), and in co-operation with the Communications Security Establishment (CSE) of the Government of Canada. A list of validated products is maintained by NIST and is available on the Web site listed at the end of this bulletin.

Reference: http://csrc.nist.gov/cryptval/140-1.htm

Annex B. Existing standards and definitions

ISO/IEC 7498-2: OSI Basic Reference Model – Security Architecture

This standard contains the following basic and important definitions:

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.

There is no explicit statement in the standard that a digital signature shall be based on public key cryptosystem, but the digital signature mechanism is described as follows:

The **digital signature mechanisms** define two procedures:

a) signing a data unit; and

b) verifying a signed data unit

The first process uses information which is private (i.e. unique and confidential to the signer). The second process uses procedures and information which are publicly available but from which the signer's private information cannot be deduced.

NOTE: This definition is thus very general, and fits the Directive very well, without imposing any technical restrictions.

Repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication

Data origin authentication: The corroboration that the source of data received is as claimed.

Non-repudiation with proof of origin: The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.

Non-repudiation with proof of delivery: The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

ISO/IEC 10181-4 OSI Security frameworks for open systems: Overview

This standard explains many important concepts, such as trusted third parties, security certificates and security tokens.

ISO/IEC 10181-4 OSI Security frameworks for open systems: Non-repudiation framework

This standard refines and extends the concepts of the non-repudiation services described in ISO/IEC 7498-2. It contains the following important definitions:

Evidence: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

A **non-repudiation policy** may include the following:

- Rules for the generation of evidence, e.g. specification of the classes of activity for which Non-repudiation evidence should be generated; specifications of the Trusted Third Parties (TTPs) to be used to generate evidence etc.
- Rules for the verification of evidence, e.g. specifications of the Trusted Third Parties (TTPs) whose evidence is acceptable; for each Trusted Third Party (TTP), the forms of evidence that will be accepted from that Trusted Third Party (TTP).
- Rules for the storage of evidence.

ISO/IEC 13888 Security techniques – Non-repudiation

Part 1 of this standard defines in detail a number of additional concepts in relation to non-repudiation. It also specifies evidence generation and verification mechanisms:

Non-repudiation policy: A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.

Non-repudiation token: A special type of security token as defined in ISO/IEC 10181-1 consisting of evidence and optionally, of additional data.

Part 3 of this standard defines specific tokens and mechanisms using asymmetric techniques.

ISO/IEC 14888 Security techniques – Digital signatures with appendix

This multipart standard specifies several digital signature mechanisms with appendix for messages of arbitrary length. The mechanisms are based on asymmetric cryptographic techniques.

The verification of a digital signature requires the signing entity's verification key. It is thus essential for a verifier to be able to associate the correct verification key with the signing entity. IF this association is not inherent in the verification key itself, but provided by other means, the scheme is then said to be »certificate-based».

ISO/IEC 9594-8 (X.509): OSI – The Directory – Authentication Framework

This very important standard defines the X.509 certificate, but contains also important reference material for the use of certificates for strong authentication. The standard contains the following basic definitions:

User certificate; public key certificate; certificate: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.

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. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range

ETSI Draft TR 101 xxx: Telecommunications Security: Electronic Signature

Standardization Report

ETSI SEC has made the following draft definition:

Electronic Signature: Evidence in a digital form than can be processed to get confidence that some commitment has been explicitly endorsed under a signing policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally a role.

Annex C - MAPPING ANNEX II TO EXISTING STANDARDS

This Annex contains a comparison of the requirements, identified in Annex II of the directive, for CSPs issuing qualified certificates, with BS7799 and RFC 2527. The requirements in Annex II are:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and secure and immediate revocation service;

(c) ensure that the date and time, when a certificate is issued or revoked, can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel which possesses the expert knowledge, experience, and qualifications necessary for the offered services, in particular competence at the managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also exercise administrative and management procedures and processes which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the processes supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification service provider generates signature creation data, guarantee the confidentiality during the process of generating that data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in this Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature creation data of the person to whom the certification service provider offered key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature, inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes
- information can be checked for authenticity
- certificates are publicly available for retrieval in only those cases for which the certificate-holder’s consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

C.1 Annex II and BS 7799

Annex II	BS 7799
General applicability	BS 7799 is concerned with general information security management in general. It does not address specific concerns relating to Certification Service Providers. BS 7799-1 describes general codes of practice for security which gives guidance but does not identify specific requirements. BS 7799-2 specifies requirements for information security management. By being accredited to BS 7799-2, directive requirements in a given area may be assumed to have been met as indicated below. Where it is indicated that an area is not specifically addressed, the general risk analysis requirements of BS 7799-2 could lead to the appropriate controls even though they are not specifically identified in BS 7799.
A. reliability	General security management system: Part 2 section 3 and security controls contribute to the reliability of CSP Part 1 all sections Part 2 section 4. Business continuity management controls: Part 1 section 9 Part 2 section 4.9
B: directory & revocation	Not specifically addressed.
C: cert. & CRL time	Covered in general terms by monitoring event logs and clock synchronisation Part 1 section 7.7 Part 2 section 4.7.7 CSP specific log requirements not addressed by BS 7799.
D: identify & attrib.	Not specifically addressed.
E: personnel i) expertise ii) administration	i) Personnel security: Job definition and resourcing, User training: Part 1 sections 4.1 and 4.2 Part 2 sections 7.4.1 and 7.4.2 ii) All of BS 7799. Of particular relevance, operational procedures and responsibilities: Part 1 section 6.1 Part 2 section 4.6.1
F: trustworthy system	Not specifically addressed.
G: forgery cert. & confid. Priv. Key	Not specifically addressed.
H: financial resources, liability insurance	Not specifically addressed.
I: Record certificate related data	Not specifically addressed.
J: not copy user sign. Creation data	Not specifically addressed.

C.2 Annex II and RFC 2527

Annex II	RFC 2527 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework)
General applicability	RFC 2527 provides a framework for CSPs to specify their practices and policies. It does not place specific requirements (cf. BS 7799-2) and only gives vague guidance (cf. BS 7799-1) on CSP practices. Where it is indicated that a topic is covered, it is only in as much as a CSP states its practices relating to this area; NOT that by following RFC 2527 the CSP has necessarily met the requirements of the Directive in this area.
A. reliability	Partially covered under: 4.2.3 financial responsibilities, 4.4.8 Compromise and Disaster recover
B: directory & revocation	4.2.1 Obligation (CA obligations) 4.2.6 Publication and repositories 4.4.4 Certificate suspension and revocation
C: cert. & CRL time	4.4.5 Security Audit Procedures
D: identify & attrib.	4.3.1 Initial registration
E: personnel i) expertise ii) administration	5.3 Personnel controls
F: trustworthy systems	4.6 Technical security controls
G: forgery cert. & confid. Priv. Key	4.4.2 Certificate issuance 4.6.2 Private key protection
H: financial resources, liability insurance	4.2.2 Liability 4.2.3 Financial responsibility
I: Record certificate related data	4.4.5 Security Audit Procedures
J: not copy user sign. Creation data	4.6.2 Private key protection

Annex D. Initial Recommendation for use of X.509 Certificates as Qualified Certificates

The following table identifies the EESSI initial recommendations for addressing the requirements on the contents of Qualified Certificates given in Annex I of the Directive and the use of the X.509 standard certificate structure.

Directive Annex I Requirement	**EESSI Initial Recommended Use of X.509 Certificate Fields (as defined in X.509 (1993) and RFC 2459)**
(a) an indication that the certificate is issued as a qualified certificate;	Either: a) Certificate Policy identifier which identifies a standarized "Certificate Policy for CSPs issuing Qualified Certificates", or b) Certificate policy qualifier which indicates that a CSP defined certificate policy incorporates the rules of the standardized "Certificate Policy for CSPs issuing Qualified Certificates".
(b) the identification and the country of establishment of the certification service provider issuing it;	Country attribute in Issuer Name
(c) the name of the signatory or a pseudonym which shall be identified as such;	A "true name" can be specified in one of the following ways: a) In subject Name or b) In subject alternative name containing the PersonalData field (as defined in "Internet X.509 Public Key Infrastructure Qualified Certificates", currently Internet Draft <draft-ietf-pkix-qc-00.txt>) A pseudonym can be specified in one of the following ways: a) In Subject Name indicated by prefixing CommonName with "Pseudonym: " e.g. CN= "Pseudonym: Beethoven" , or b) In Personal data indicated by use of the pseudonym attribute (as defined in the above Internet draft).
(d) provision for a specific attribute of the holder to be included if relevant, depending on the purpose for which the certificate is intended;	Subject attributes may be held either as: a) attributes within the Distinguished Name b) certificate extensions

(e) a signature verification data which corresponds to a signature creation data under the control of the holder;	Subject public key info
(f) beginning and end of the period of validity of the certificate;	Validity
(g) the identity code of the certificate;	Issuer name and certificate serial number
(h) the advanced electronic signature of the certification service provider issuing it;	The signature value of the certificate
(i) limitations on the scope of use of the certificate, if applicable; and	Key usage and extended key usage extensions
(j) limits on the value of transactions for which the certificate can be used if applicable.	This can be specified for example using either: a) a certificate extension b) a policy qualifier previously defined in a well-known certificate policy