Certification Authority in Praxis. Security Aspects.

Jaroslav Pinkava
jaroslav.pinkava@normancz.cz

Norman Data Defense Systems
Czech Republic

Abstract

There are many problems connected with practical implementation of certification authority. Correspondent solutions have to answer the questions related with applied software, with technical aspects, with administration basis, and with human factor. Most answers to these questions are described in documents such as Certification Policy and Certification Practice Statement.

In this work will be presented an introductory overview of the most important security character problems tied with functionality of certification authority.

Firstly - the cryptographic side of the discussed solution. There are several different important parts of this problem: The cryptography implemented by CA (signature creation devices, protection of CA signing key), the basic key generation procedure, and the cryptography implemented on the user side (for signature creation). All of the parts exist in particular environment and their use is defined by particular policy. Some important properties of used cryptographic modules are described in forthcoming European standards in this area (ETSI, CEN/ESSI).

Second - the cryptography is not the only side of the security problems connected with implementations of certification authority. The RFC2527 document: Certificate Policy and Certification Practices Framework has defined the basics for describing the structure of most parts of policy used by CA. Some of these specifications (for example Physical, Procedural, and Personnel Security Controls) describe other security aspects.

The connected problems are at this time solved by preparated standards by EESSI following the ideas from European Directive on Electronic Signatures. There are two bodies participating on this work – ETSI and CEN/ISSS.

The goal of the presented article is to take a look at close connections between all the mentioned security aspects and necessity of their serious consideration. This will be done through the overview of standards preparated by CEN/ISSS and some comments.

Keywords: certification authority, security, certification practice statement, European standards

1. Introduction

Firstly – we take a look on some basic notions as certification policy and certification practice statement (section 2). Shortly are mentioned security problems connected with CA functioning. Then will be given an overview of forthcoming European standards. The main interest is on prepared security standards CEN/ISSS. As the article focus is on description of forthcoming standards, they are offen used citations from these prepared EU documents.

2. Certification Policy and Certification Practice Statement

The purpose of common used standard - rfc.2527 is to establish a clear relationship between certificate policies and CPSs, and to present a framework to assist the writers of certificate policies or CPSs with their tasks. The CP aand CPS are here defined on following way:

Certificate policy (CP) - 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.

Certification Practice Statement (CPS) - A statement of the practices which a certification authority employs in issuing certificates.

The X.509 standard defines a certificate policy 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"[ISO1]. An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

A certificate policy, which needs to be recognized by both the issuer and user of a certificate, is represented in a certificate by a unique, registered Object Identifier. The registration process follows the procedures specified in ISO/IEC and ITU standards. Theparty that registers the Object Identifier also publishes a textual specification of the certificate policy, for examination by certificate users. Any one certificate will typically declare a single certificate policy or, possibly, be issued consistent with a small number of different policies.

Certificate policies also constitute a basis for accreditation of CAs. Each CA is accredited against one or more certificate policies which it is recognized as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon accreditation with respect to the certificate policies involved). The assessed set of certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these certificate policy indications in its well-defined trust model.

The following extension fields in an X.509 certificate are used to support certificate policies:

- Certificate Policies extension;
- Policy Mappings extension;
- Policy Constraints extension.

The term certification practice statement (CPS) is defined by the ABA Guidelines as: "A statement of the practices which a certification authority employs in issuing certificates." [ABA1]

In the 1995 draft of the ABA guidelines, the ABA expands this definition with the following comments:

A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration.

Certain forms for legally implementing certification practice statements lend themselves to particular relationships. For example, when the legal relationship between a certification authority and subscriber is consensual, a contract would ordinarily be the means of giving effect to a certification practice statement. The certification authority's duties to a relying person are generally based on the certification authority's representations, which may include a certification practice statement.

Whether a certification practice statement is binding on a relying person depends on whether the relying person has knowledge or notice of the certification practice statement. A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents incorporated into the certificate by reference. It is therefore advisable to incorporate a certification practice statement into a certificate by reference.

As much as possible, a certification practice statement should indicate any of the widely recognized standards to which the certification authority's practices conform. Reference to widely recognized standards may indicate concisely the suitability of the certification authority's practices for another person's purposes, as well as the potential technological compatibility of the certificates issued by the certification authority with repositories and other systems.

The concepts of certificate policy and CPS come from different sources and were developed for different reasons. However, their interrelationship is important.

A certification practice statement is a detailed statement by a certification authority as to its practices, that potentially needs to be understood and consulted by subscribers and certificate users (relying parties). Although the level of detail may vary among CPSs, they will generally be more detailed than certificate policy definitions. Indeed, CPSs may be quite comprehensive, robust documents providing a description of the precise service offerings, detailed procedures of the life-cycle management of certificates, and more - a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.

Although such detail may be indispensable to adequately disclose, and to make a full assessment of trustworthiness in the absence of accreditation or other recognized quality metrics, a detailed CPS does not form a suitable basis for interoperability between CAs operated by different organizations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards and common assurance criteria on an industry-wide (or possibly more global) basis. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, multiple different CAs, with non-identical certification practice statements, may support the same certificate policy.

The certificate policy definition will be a broad statement of the general characteristics of that certificate policy, and an indication of the types of applications for which it is suitable for use. Different departments or agencies that operate certification authorities with different certification

practice statements might support this certificate policy. At the same time, such certification authorities may support other certificate policies. The main difference between certificate policy and CPS can therefore be summarized as follows:

(a) Most organizations that operate public or inter- organizational certification authorities will document their own practices in CPSs or similar statements. The CPS is one of the organization's means of protecting itself and positioning its business relationships with subscribers and other entities.

(b) There is strong incentive, on the other hand, for a certificate policy to apply more broadly than to just a single organization. If a particular certificate policy is widely recognized and imitated, it has great potential as the basis of automated certificate acceptance in many systems, including unmanned systems and systems that are manned by people not independently empowered to determine the acceptability of different presented certificates.

In addition to populating the certificate policies field with the certificate policy identifier, a certification authority may include, in certificates it issues, a reference to its certification practice statement.

A set of provisions is a collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework. A certificate policy can be expressed as a single set of provisions. A CPS can be expressed as a single set of provisions with each component addressing the requirements of one or more certificate policies, or, alternatively, as an organized collection of sets of provisions. For example, a CPS could be expressed as a combination of the following:

(a) a list of certificate policies supported by the CPS;

(b) for each certificate policy in (a), a set of provisions which contains statements that refine that certificate policy by filling in details not stipulated in that policy or expressly left to the discretion of the CPS by that certificate policy; such statements serve to state how this particular CPS implements the requirements of the particular certificate policy;

(c) a set of provisions that contains statements regarding the certification practices on the CA, regardless of certificate policy.

This framework outlines the contents of a set of provisions, in terms of eight primary components, as follows:

- Introduction;
- General Provisions;
- Identification and Authentication;
- Operational Requirements;
- Physical, Procedural, and Personnel Security Controls;
- Technical Security Controls;
- Certificate and CRL Profile; and
- Specification Administration.

Components can be further divided into subcomponents, and a subcomponent may comprise multiple elements.

In rfc.2527 is given checklist or (with some further development) a standard template for use by certificate policy or CPS writers. Such a common outline will facilitate:

(a) Comparison of two certificate policies during cross-certification (for the purpose of equivalency mapping).

(b) Comparison of a CPS with a certificate policy definition to ensure that the CPS faithfully implements the policy.

(c) Comparison of two CPSs.

3. Short overview of security problems connected with CA functioning

Issuing CA to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival must use non-technical security controls of following 3 types (rfc 2527):

- Physical Security Controls (Site location and construction; Physical access; Power and air conditioning; Water exposures; Fire prevention and protection; Media storage; Waste disposal; and Off-site backup)
- Procedural Controls (requirements for recognizing trusted roles)
- Personnel Security Controls (personnel filling the trusted roles, contracting personnel)

The technical security controls define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). The problematic can be divide in following sections:

- Key Pair Generation and Installation;
- Private Key Protection;
- Other Aspects of Key Pair Management;
- Activation Data;
- Computer Security Controls;
- Life-Cycle Security Controls;
- Network Security Controls; and
- Cryptographic Module Engineering Controls.

4. Forthocoming EU Standards

There are two basic workgroups preparing standards by recommendation of EESSI (European Electronic Signatures Standardisation Initiative) : ETSI and CEN/ISSS. We will give only shortly overview of documents of first group (ETSI) and will concentrate our phocus on the standards prepared by CEN/ISSS. The documents prepared by European forthcoming standards – ETSI group are:

In the first phasis of the work was prepared programme document Electronic Signature Report (http://docbox.etsi.org/tech-org/security/open/el-sign/ESRep042.pdf) . The second phase started in beginning of the year 2000 and in this year are elaborated following four documents:

- **Policy Requirements for CSPs Issuing Qualified Certificates;**
- **Qualified Certificates Profile;**
- **Time Stamping Profile;**
- **Electronic Signature Formats.**

In the year 2001 ETSI will prepare following documents:

- **Security management and policy requirements for CSPs issuing time stamps**
- **Policy requirements for CAs issuing other than Qualified Certificates**
- **Policies for CSP's**
- **Electronic Signature syntax and encoding formats in XML**
- **Technical aspects of signature policies (Informative annex to TS 101 733)**
- **Infrastructure and interoperability requirements for provision of status information on Certification Service Providers**

5. Forthcoming EU standards – CEN/ISSS

5.1. Area D

The document in preparation is called Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures (draft N142, Version 0.9, March 2001) This CEN Workshop Agreement (CWA) is about security requirements on products and technology components, used by CSPs, to create Standard and Qualified Cerificates.

Main focus of this standard is on Annex II of European Directive on Electronic Signatures: Description of a Certification Service Provider System. Two distinct areas are described: core functionality and supplementary functionality.

The *core services* a CSP MUST provide are:

Registration Service: Verifies the identity and, if applicable, any specific attributes of a Subscriber. The results of this service are passed to the Certificate Generation Service.

Certificate Generation Service: Creates and signs Certificates based on the identity and other attributes of a Subscriber as verified by the Registration Service.

Certificate Dissemination Service: Disseminates Certificates to subscribers, and if the Subscriber consents, to Relying Parties. This service also disseminates the CA's policy and practice information to Subscribers and Relying Parties.

Revocation Management Service: Processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.

Revocation Status Service: Provides Certificate revocation status information to relying parties. This service MAY be a real-time service or MAY be based on revocation status information which is updated at regular intervals.

The *supplementary services* a CSP MAY provide are:

Subscriber Signature-Creation Device Provision Service: Prepares and provides a Signature Creation Device (SCD) to Subscribers.

Note: examples of this service are:

• A service which generates the subscriber’s key pair and distributes the private key to the subscriber;

• A service which prepares the subscriber’s Secure Signature Creation Device (SSCD) and device enabling codes and distributes the SSCD to the registered subscriber.

Time Stamp Service: A third party, trusted to provide a Time Stamp Service. The Time Stamp Service provides proof that a data item existed before a certain point in time (proof of existence). If the data item has been signed by the requester before being submitted to the Time Stamp Authority (TSA), then the Time Stamp Service provides proof that the data item existed and was in possession by this entity before a certain point in time (proof of possession). A Time Stamp Service involves two basic operations:

- A time stamping process, which cryptographically binds time values to data values, and,
- A time stamp verification process, which evaluates the correctness of those bindings.

A TSA provides the time stamping service, whereas the time stamp verification process MAY involve other trusted authorities.

There are desribed (in the standard) specification about security requirements applicable

- to both Standard and Qualified Certificates
- for CSPs only issuing Standard Certificates
- for CSPs issuing Qulified Certificates

The security requirements are divided on:

- CSP general functionality and security requirements
  1. Management
  2. Systems and Operations
  3. Identifiaction and Authentification
  4. Key Management (functional and security requirements)
  5. Accounting and Auditing
  6. Archiving
  7. Backup and Recovery
- CSP core services functionality and security requirements
  1. General
  2. Registration Service
  3. Certificate Generation Service (functional and security requirements)
  4. Certificate Dissemination Service
  5. Certificate Revocation management Service
  6. Certification Revocation Status Service (functional and security requirements)
- CSP supplementary services functionality and security requirements
  1. Time Stamping Service (functional and security requirements)
  2. Subscriber Signature Creation Device (SCD) Provision Service

5.2. Area F

Area F was charged with developing a standard for secure signature creation devices (SSCDs) that fulfils the requirements of Annex III of the EU Electronic Signatures Directive, in accordance with the Work Programme of the European Electronic Signatures Standardisation Initiative (EESSI)- document N118. At now there exists no consensus in this area. Two key issues motivated the companies that opposed the standard. First, a number of companies felt that the proposed security assurance requirements were too high. Second, several companies opposed the inclusion of “Type 1” SSCDs in the standard.

The EvaluationAssurance Level (ALE) indicates how the security functions claimed by a product have been verified in accordance with the Common Criteria (ISO IS 15408), a shared language for defining security and a method of accepting evaluations across national boundaries. In other words, the ALE represents the level of confidence one has regarding the security of the product. The Area F Project Team included an EAL of 4 with two augmentations in its proposed standard. As differences over this issue blocked consensus, the Workshop decided to forward two standards to the EESSI Steering Board – one with EAL 4 and the other with EAL 4 plus.

The Type 1 SSCD is a device that generates the signature creation data that is then exported to a user’s personal signing device, such as a smart card. Several companies at the Brussels meeting asked for the Type 1 SSCD be removed from the standard. These companies felt that the standards for the Type 1 SSCD fell within the scope of the work being undertaken by Area D, which is addressing trustworthy systems used by certification authorities. No objections against

the security requirements in the protection profile were raised. The Expert Group views the inclusion of the Type 1 SSCD only as one alternative for signature creation data generation.

Both versions have an analogic structure of their contents (last documents versions are N136 and N137, March 2001). The aim of the effort to standardise the security requirements for SSCDs is to ensure their conformity with the EU Directive and their mutual interoperability. The presented CWA defines a Protection Profile (PP) according to the Common Criteria for a SSCD containing SCD and relating to signature-verification data (SVD) in the corresponding certificate. Document specifies the security requirements for a SSCD which is the TOE (The Object of Evaluation). The TOE is represented by the SSCD including SCD/SVD generation, SCD storage, and signature-creation functionality. Although it is possible that the TOE includes additional functionality, such as the signature-creation application (SCA) or the certification generation application (CGA), the PP assumes the SCA to be part of the immediate environment of the TOE. The SSCD security requirements also include a minimum set of requirements to be fulfilled by the signature algorithms and their parameters allowed for use with SSCDs.

The main part of both documents is Annex A – Protection Profile for the SSCD, which follows the rules and conventions laid out in Common Criteria 2.1 (part 1, Annex B – Specification of Protection profiles). Admissible algorithms and parameters for algorithms for secure signature-creation devices (SSCD) are given in a separate document.
The Annex A is organized in following sections:
Section 1 provides the introductory material for the Protection Profile.
Section 2 provides general purpose and TOE description.
Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.
Section 4 defines the security objectives for both the TOE and the TOE environment.
Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied by the TOE.
Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

5.3. Area G

First document in this area is Security Ruquirements for Signature Creation Systems (last draft N141, March 2001, version 3.9). This standard specifies security requirements and recommendations for Signature Creation Applications. First part contain the definitions, modelling and technical introductions to the Signature Creation Application and the operational environment that are necessary to support the specification of security requirements. The second part specifies the security requirements and recommendations for each functional component of a Signature Creation Application together with rationale.

Document supports the EU directive for electronic signatures. It specifies security requirements for Signature Creation Applications that create Advanced Electronic Signatures with the help of a

Secure Signature Creation Device and Signer´s Signature Creation Data using Qualified Certificates, by means of the following:

- providing a model of the Signature Creation Environment and a functional model of Signature Creation Applications;
- specifying overall requirements that apply across all of the functions identified in the functional model;
- specifying Security Requirements for each of the functions identified in the Signature Creation Application excluding the Secure Signature Creation Device.

A Signature Creation Application is intended to deliver a Qualified Electronic Signature associated with a Signer's Document as a Signed Data Object to the user or some other application process in a form specified by the user. A further goal is to provide a specification so that applying an electronic signature is as easy and error-free as applying a hand written signature. It should be possible for all people, including people with special needs to create an electronic signature. Achieving these goals will contribute to consumer confidence and trust in electronic signatures. This specification is intended to be independent of particular technologies and realisations that might be employed in products. The following aspects are considered to be out of scope:

- generation and distribution of Signature Creation Data (keys etc.), and the selection and use of cryptographic algorithms;
- the legal interpretations of any form of signatures (e.g. the implications of countersignatures, multiply signed documents and signatures covering complex information structures containing other signatures).

This standard specifies security requirements that are intended to be followed by implementors of SCAs. The primary functions of the SCA are contained in a set of 'Trusted' and 'Applications Specific' SCA components. The trusted components are all mandatory if not marked otherwise and are relevant for every SCA (DHC and SAC are always considered to be present in order to encourage compatibility of the SCA with the widest possible population of SSCDs). The application specific components are application context dependent, i.e. their presence, construction and functionality is application specific.

The **trusted** SCA components are:

SDP - Signer´s Document Presentation Component used for presenting the Signer´s Document that the signer selects by the Signer Interaction Component.

SAV - Signature Attributes Viewer used for viewing the Signature Attributes that the signer selects by the Signer Interaction Component and which will be signed together with the Signer's Document. The SAV will include a capability to present the major components of the possibly application specific Signer's Certificate Content.

DTBSF – Data To Be Signed Formatter which formats and sequences the Signer´s Document or a hash of it together with the Signature Attributes and delivers the result to the Data Hashing Component.

SIC - Signer Interaction Component over which the signer interacts with the SCA to control the signature creation process, and over which the SCA returns error and status messages to the signer. This interface is used for all interactions between the Signer and the SCA, including input/selection of the Signer's Document and Signature Attributes except the Signer´s Authentication Data.

SAC - Signer´s Authentication Component (e.g. a card terminal with PIN pad). This is used for presenting knowledge based Signer´s Authentication Data and/or biometric features and

preparation of the Signer´s Authentication Data in such a way that they can be compared with Signer´s Authentication Data held in the SSCD.
DHC - Data Hashing Component for producing the DTBS Representation (which might be non-hashed, partially hashed or completely hashed as required by the SSCD). If the SSCD carries out all of the hash processing, then the task of this component is only to forward the DTBS Representation unchanged to the SSCD.
SSC - SSCD/SCA Communicator which manages the interaction between SCA and SSCD.
SSA - SSCD/SCA Authenticator which establishes a trusted path between SSCD and SCA. The presence of this component is conditional, i.e. it might only present in SCAs that are under the control of public service providers and where the trusted path cannot be established by organisational means.
The **application specific** components may include the following:
SDC - a Signer's Document Composer (e.g. a text editor) for creation, input or selection of the signer's document. The information that this acts on is managed through the SIC.
SDOC - a Signed Data Object Composer that usually takes the DTBSF components and associates them with the bit string representing the electronic signature as delivered by the SSCD, and outputs the result (i.e. the SDO) of the signing process in some standard format as specified by the SDO Type (e.g. as specified in the ETSI Electronic Signature Formats Document).
SLC - a Signature Logging Component that records some details of the most recent signatures created by the SCA.
CSPC - a Certification Service Provider Interaction Component which is used e.g. for retrieving the signer´s certificates (if not stored in the SSCD) or for obtaining a time stamp where required by the security policy.
SHI - SSCD Holder Indicator that is used for displaying the SSCD holder´s name.
Examples of devices which may support an SCA are PCs, Laptops, Palmtops/PDAs and Mobile Phones.

The second document in this area is Procedures for Electronic Signature Verification (last draft **N 140**, March 2001, version 1.0.5). Signature verification is a process that can be performed in many ways, for example:

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

The term "displayed" (in Directive) should be interpreted in a more general sense as "presented", since the signed data may be any type of media (text, sound, video etc). Primary purpose of document is to provide guidance on the way to verify qualified electronic signatures that are equivalent to manual signatures according to the chapter 5.1. from the Directive and to explain the importance of the use of time-stamping and/or time marking for the a later verification of the signature. However, it may also be used when the certificate of the signer is not a Qualified Certificate.

The Signature Policy is one of central notions in this document. When two independent parties want to evaluate an electronic signature, it is necessary that they use the same rules in order to get the same result. It is therefore important that the signature policy chosen by the signer must be unambiguously available to the verifying parties. A signature policy may be issued, for example, by a party relying on the electronic signatures and selected by the signer for use with that relying party. Alternatively, a signature policy may be established through an electronic trading association for use amongst its members. Both the signer and verifier use the same signature policy.

The signature validation policy specifies the technical rules to be followed by the signer and the verifiers used to process the electronic signature. This rules allow for the initial and usual verifications of electronic signatures issued under that form of signature policy.

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

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

Usual Verification that may be done years after the electronic signature was produced, does not need to capture more data than the data that was captured at the time of initial verification. However there is one exception: if the cryptography that was used years before is likely to be broken soon, at that stage more information needs to be gathered in order to extend the life-time of the cryptography.

An electronic signature may exist in many forms including:

- an Electronic Signature (ES), which includes the digital signature and other basic information provided by the signer. The ES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures. It provides basic authentication and integrity protection and can be created without accessing on-line (time stamping) services. However, without the ability to position the electronic signature in a time scale, the digital signature does not protect against the threat that the signer later denies having created the electronic signature at a time the corresponding certificate was valid and not revoked (i.e. it does not provide non-repudiation);
- an ES with Time (ES-T), which either adds a **Time Stamp** from a Time Stamping Authority to the Electronic Signature, to take initial steps towards providing long term validity, or adds **Time Mark** to the Electronic Signature, by copying both the Electronic Signature and the Time Mark in a secure audit trail;
- an ES with Complete validation data (ES-C), which adds to the ES-T the references to (but not the values of) the complete set of data supporting the validity of the electronic signature (e.g. certification path and revocation status information). The ES-C thus contains both the references of the validation data *and their hash values*. This allows to make sure that the actual values which has been captured are the one's referenced. The complete set of data supporting the validity of the electronic signature does not necessarily need to be kept together with the Electronic Signature but may be kept somewhere else. The ES-C is the common denominator of two other forms of ES. One form (identical to the ES-C) allows to store these values elsewhere, e.g. in some central storage, while the other form (ES-X) allows to store all the values of the validation data together with the ES.

The output status of the initial verification process can be:

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

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

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

the application or user, thus allowing the application or user to decide what to do with partially correct electronic signatures.

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

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

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

then the values of these elements may be added to the ES-C. This form of extended validation data is called ES-X.

An electronic signature SHALL be valid when:

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

An **initial** signature verification system is composed of :

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

A **usual** signature verification system is composed of :

- the secure signature verification process,
- an interface to enter the signer's document and to select the electronic signature to be validated (there may be more than one electronic signature attached with the user data),
- a display/sound/video interface to present (e.g. display, listen to or visualize) the signer's document with the right format,
- an interface to present the Signature Policy;
- an interface to get the signer information and the output status after the initial signature verification,
- an optional interface to enter the recording time of the electronic signature from the secure audit trail of an independent Trusted Third Party;
- an optional interface to get the definition of the Signature Policy (when the initial signature

verification system is not only support dynamically programmable signature policies).

Verification can be performed by human, machine or Third-Party. Four main environments have been considered: the home environment, the office environment, the public environment and the mobile environment.

All components of the signature verification system that interact with the Secure Signature Verification Process should be realized in a Secure Area - this is an area within a component in which the storage and processing of data and the processes within this area are protected against successful manipulation by means of special measures.

In the document are mentioned some other questions (Conformity Assessment, Legal aspects, Multiple Signatures and Archive systems).

5.4. Area V

Document prepared in this area is called EESSI Conformity Assessment. His purpose is to provide quidance with a view to harmonize the application of the standards for services, processes, systems and products for Electronic Signatures developed under the European Electronic Signature Standardization Initiative (EESSI) by the CEN/ISSS Workshop on Electronic Signatures and ETSI SEC ESI Working Group. The Guidance is intended for use by Certification Service Providers, manufacturers, operators, indenpendent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to these standards.

The EESSI Conformity Guidance will be issued in five parts:

Part 1. – General
Part 2. – Certification Authority services and processes
Part 3. – Trustworthy systems managing certificates for electronic signatures
Part 4. – Signature creation applications and procedures for electronic signature verification
Part 5. – Secure signature creation devices.

At this time there exist drafts for only first two parts. The first part (draft N143, March 2001) is common description of the problematics.

The second part (draft N144, March 2001) is Guidance on Conformity Assessment of Certification Authority services and processes (against the standard ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates). The publication specifies guidance, the observance of which is intented to ensure that assessors of independent bodies operate in a consistent and reliable manner, thereby facilitating their acceptance on a national and international basis. The guidance is based upon the applicable documents in the EN 45000 series of standarts and the relating guidelines published by the European co-operation for Accreditation (EA). In particular has been taken into account EA document EA-7/03, providing guidelines for the bodies operating certification of Information Security Management Systems. Conformity assessment of Cas is voluntary.

In document are given requirements for independent bodies, qualification criteria for individual assessors, Code of a Conduct for assessors, assessment team competence and use of technical experts. The guidance on the conformity assessment process describes stages of the assessment. The rest of the document is on use of ETSI TS 101 456.

At this time (March 2001) start work on following two documents:

5.5 New areas in 2001

Area AA: Extension of SSCD requirements towards specific applications/environments and towards e-commerce applications - Art5.2

Scope: To broaden the requirements for SSCD towards:
- non-generic SSCD profiles for the implementation in specific applications (e.g. personal data assistants, mobile phones) and the operation in specific environments (e.g. public terminals);
- protection profiles in response to Art 5.2 of the Electronic Signature Directive to address specifically the requirements of electronic commerce.

The SSCD PP has been based on the working assumption of a general technology-neutral approach that has solely been based on the requirements that are defined by the Directive. Whilst this allows for swift and harmonised realization of the Directive in an implementation-independent manner, a side-effect is that the general SSCD-PP neither could emphasize strengths of any certain technology promising to be capable to deploy electronic signatures, nor could the value-added of employing CC-evaluated SSCDs in e-commerce areas (referred to as is5.2 signaturesld) be sufficiently addressed. With reference to the concluding area F presentation in Brussels, 21 st November 2000, the SSCD PP may well be the basis of future directions or further PPs may be established. As illustrated in the following figure, three such possible directions have been identified.
1. Special SSCDs that pay attention to specific technological instantiations: The envisaged components are mobile phones and personal digital assistants (PDAs) Š referred to as iohandheld COTS SSCDld in the context of this proposal.
2. e-commerce scenarios: Related to the broad deployment already achieved by the technologies mentioned above, employing these technologies for signature-creation based on article 5.2 of the Directive may well benefit from the trust established by CC evaluation. Although such evaluation is not mandated by Directive, it is considered a potential trust-enabler. Therefore, a PP streamlined to the requirements in the e-commerce area is planned.
3. Specific environments: Finally, specific environments the SSCD is operated in are addressed. The aim is to specify a PP for SSCDs used together wit public terminals. The aim is to cover environments such as for instance are expected to be in place in public administrations in transitional stages from conventional paper-based to electronic administration.

Area K: Requirements for smart cards used as SSCD

Scope: Area F has concluded that an assurance level of EAL4+ is in any case sufficient for a SSCD, (secure signature-creation device) in the end-user environment. Smart cards are a means to reaching an EAL 4+ assurance level.
This work will identify functional specifications of a smart card to be used as SSCD in a PKI with a signature policy to be defined, and to define the associated manufacturing and personalisation process. A WAP mobile based PKI is suggested to be an initial example case, if collaboration with WAP forum will be possible. This can also be a PKI compatible with state of the art PKIX standardisation.

Based on that PKI, a user owning a smart card, specified according to our task must be able to send his electronic signature to a server, electronic signature with legal effect as required by chapter 5.2 of the Directive.

Anyway, a basis of work could be the WIM. Exam of extends, eventually removals must be carefully done. WIM specification is mainly based on standards 7816_8 for cryptographic commands and on PKCS15 for data structuring.

The object of activity is verifying if state of the ISO7816_8 is complete enough to specify card commands and if object identifiers required by signature constraints must be added to PKCS15. Functional specifications will carefully take into account key generation , key introduction, key renewal, certificate introduction phases and the associated access conditions.

Specific attention must be paid to manufacturing process and personalisation process in order to eventually adapt procedures of secret key and personal data introduction. Relationship (key sharing) between manufacturers and future CA must be defined as well.

6. Final remarks

As the security aspects of CA activities are at this moment very thoroughly discussed in prepared EU standards, we take a short look on this documents. The most of overviewed documents are not finalized. There is a lot of a work to do. But the present materials can show the content and complexity of the problematics and show the directions for the work both in theory and practice.

7. References

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

[2] IETF RFC 2527 (1999): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", S. Chokhani, W. Ford.

[3] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: authentication framework".

[4] FIPS PUB 140-1 (1994 January 11): "Security Requirements For Cryptographic Modules".

[5] ETSI TS 101 862: "Qualified certificate profile".

[6] ISO/IEC 15408 :1999 Information technology - Security techniques - Evaluation criteria for IT security (parts 1 to 3).

[7] CEN/ISSS – drafts in preparation: http://www.ni.din.de/index.php3

There are much more relevant documents, articles, standards, drafts etc. The citations can be found for example in prepared drafts [7].