ETSI TR 102 206 V1.1.3 (2003-08)

Technical Report

Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework

Reference

DTR/M-COMM-005

Keywords

commerce, electronic signature, M-commerce, mobile, security, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project M-Commerce (M-COMM).

Introduction

Citizens around the world are making use increasingly of electronic communications facilities in their daily lives. This often involves interactions between parties who have never previously met - or may never meet - and for whom no pre-established relationship exists. Consequently, communications networks of all kinds are being exploited in new ways to conduct business, to facilitate remote working and to create other 'virtual' shared environments.

Consumers, businesses and government departments alike benefit in various ways. For the European Union (EU), electronic commerce presents an excellent opportunity to advance its programmes for economic integration. But, such an approach requires an appropriate security mechanism to allow completion of 'remote' interactions between parties with confidence. To this end, the European Parliament and Council Directive on Electronic Signatures (1999/93/EC [12]) was published on December 13th, 1999.

The definition of 'electronic signature' contained in article 2 of the directive facilitated the recognition of data in electronic form in the same manner as a hand-written signature satisfies those requirements for paper-based data. Since electronic signatures can only be as 'good' as the technology and processes used to create them, "standardization" activities such as those in Europe by ETSI and CEN within the EESSI framework aim to ensure that a common level of confidence and acceptance can be recognized. The result will be a powerful enabling facility for electronic commerce and, more generally, for completion of transactions of any kind.

In the context of the EU Directive, the present document focuses on electronic signatures created by cryptographic means in a "secure signature creation device". As at June 2003, security provisions for signature creation and verification systems are such that parties wishing to provide a signature require 'special' equipment. Typically, this involves a smartcard and a card reader with sufficient processing power and display capabilities to present full details of the transaction to be "signed". For consumer markets, however, it is doubtful whether individual citizens will want to invest in such equipment, which for the most part may remain connected to (or inserted into) personal computer equipment located in the home.

An alternative approach is to capitalize on the fact that many citizens already possess a device which contains a smartcard and which itself is effectively a personal card reader- their mobile phone. In some European countries, mobile penetration rates are approaching 80 % of the population. As one of the most widely-owned electronic devices, the mobile phone represents the natural choice for implementation of a socially-inclusive, electronic signature solution for the majority of citizens.

Electronic signatures created in this way have become known as "Mobile Signatures" and a number of initiatives are already underway to evaluate the feasibility of such an approach. Only a small number of these have so far been implemented commercially and none have yet been extended to a mass-market scale. Many of those engaged in such activity cite 'interoperability' issues as a restraining factor, requiring standardization to avoid market fragmentation.

The concept of a "Mobile Signature" is attractive because it leverages existing commercial models, network infrastructure, mobile device technology (including the SIM-infrastructure) and customer relationships managed by GSM mobile network operators. This offers the prospect that the concept could be adopted by around one billion mobile phone users in 179 countries, world-wide. Extension of the concept to other mobile network technologies is also possible.

Adoption of mobile signature might also assist in the fight against international crimes, such as money 'laundering'. In this case, the opportunity provided by mobile signature to identify the citizens who are party to a transaction is attractive, subject to provisions concerning Data Protection, Privacy and Legal Interception (as applied to data services).

Acceptance of the concept universally now requires "standardization" of a common service methodology, where signature requests/responses can be issued/received in a 'standard' format - irrespective of mobile device characteristics. To this end, the European Commission allocated funds to ETSI to establish a Specialist Task Force (STF-221) to produce a set of deliverables on **mobile signature service**.

It is envisaged that mobile signature services will play a pivotal role in reaching an appropriate level of confidence, acceptance and interoperability to support implementation of the European Directive on Electronic Signature - particularly for consumer (mass) markets. The present document focuses on those technologies able to realize a mobile signature the equivalent of an "enhanced electronic signature" as defined by the European Directive.

The mobile signature service is considered suitable for the administration and management of all aspects relating to:

- Advising and guiding citizens about the use of mobile signature.
- Acquiring mobile signature capability.
- Managing citizen identity (including data protection and individual privacy).
- Processing of signature requests from application providers (and providing responses).
- Maintaining signature transaction records for the citizen.
- Managing all aspects of signature lifecycle (e.g. validity, expiry).
- Supporting service administration and maintenance activities.

The definition of the Mobile Signature Service comprises the following report and specifications:

- TR 102 203 [18]: "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements".
- TS 102 204 [26]: "Mobile Signature Service; Web Service Interface".
- TR 102 206 (the present document): "Mobile Signature Service; Security Framework".
- TS 102 207 [27]: "Mobile Signature Service; Specifications for Roaming in Mobile Signature Services".

Together, the TR and the TSs allow the design and implementation of interoperable mobile signature solutions.

1 Scope

The Mobile Signature Service is a service provided by a Mobile Signature Service Provider (MSSP) to a Signer and an Application Provider (AP). Because a Mobile Signature is a "universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction" (see TR 102 203 [18]), the Mobile Signature Service becomes a crucial security element within the architecture of the Application Provider itself.

In the case of transactions (e.g. financial) that rely on a Mobile Signature, the issue of liability may be raised. Both parties, i.e. the enduser and the Application Provider are willing to protect themselves from fraudulent behaviours between each other, or even from hackers, thanks to the Mobile Signature.

Without a wide and common understanding of the security considerations for Mobile Signatures by all parties (e.g. the Signer, the Application Provider etc.), it will be quite difficult for MSSPs to build commercial agreements with those parties. In this respect, it is essential for all the stakeholders to identify the level of security, a MSSP may, should, or must provide. This is the purpose of the present document.

The concept of Mobile Signatures has also to be linked with the current work of EESSI on electronic signatures taking into account the specificities of the mobile environment. TR 102 203 [18] explain that a Mobile Signature is an electronic signature that goes mobile. The present document clarifies the meaning of this sentence in the context of the security requirements of the European Directive.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] CWA 14167-1 (2001): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[2] CWA 14167-2 (2002): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

[3] CWA 14169 (2002): "Secure Signature-Creation Devices, version 'EAL 4+'".

[4] CWA 14170 (2001): "Security Requirements for Signature Creation Systems".

[5] CWA 14171 (2001): "Procedures for Electronic Signature Verification".

[6] CWA 14172-1 (2001): "EESSI Conformity Assessment Guidance - Part:1: General".

[7] CWA 14172-2 (2001): "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes".

[8] CWA 14172-3 (2001): "EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures".

[9] CWA 14172-4 (2001): "EESSI Conformity Assessment Guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification".

[10] CWA 14172-5 (2001): "EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices".

[11] CWA 14355 (2002): "Guidelines for the implementation of Secure Signature-Creation Devices".

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

[13] RSA PKCS#1 (1999): "RSA Encryption Standard".

[14] RSA PKCS#7 (1993): "Cryptographic Message Syntax Standard".

[15] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels".

[16] IETF RFC 3275: "(Extensible Markup Language) XML-Signature Syntax and Processing".

[17] ETSI SR 002 176: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

[18] ETSI TR 102 203: "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements".

[19] ETSI TS 101 456: "Policy requirements for certification authorities issuing qualified certificates".

[20] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".

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

[22] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[23] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[24] ETSI TR 102 041: "Signature Policies Report".

[25] ETSI TR 102 045: "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model".

[26] ETSI TS 102 204: "Mobile Commerce (M-COMM); Mobile Signatures; Web Service Interface Specification".

[27] ETSI TS 102 207: "Mobile Commerce (M-COMM); Mobile Signatures; Specifications for Roaming in M-signature Services".

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

[29] ETSI TS 101 181: "Digital cellular telecommunications system (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2 (3GPP TS 03.48)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

application provider: person or entity making use of Mobile Signatures created by Signers

asymmetric cryptography: means to encrypt messages in a manner that does not require from the encrypting entity to know the key used to decrypt the cipher-text

NOTE: Asymmetric cryptography also allows to sign messages in a manner that does not require from entity that verifies the signature to know the key used to produce the signature.

certification authority: authority that produces signatures on public-keys (certificates)

NOTE: The process of signing one's public-key is called "certification".

commitment type: indication of the exact intent of the electronic signature

content format: Signature Attribute that expresses the encoding of the Signer's Document

Data To Be Signed (DTBS): complete electronic data to be signed (i.e. the Signer's Document and Signature Attributes)

Data To Be Signed Formatted (DTBSF): components of the Data To Be Signed which have been formatted and placed in the correct sequence for signing according to the requirements of a Signed Data Object Type

Data To Be Signed Representation (DTBSR): data sent to a Signature Creation Device for signing

electronic signature: data in electronic form attached to, or logically associated with other electronic data and which serve as a method of authentication of that data

EU Directive: directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures

mobile signature: universal method for using a mobile device to confirm the intention of a Signer to proceed with a transaction

NOTE: In the present document, only the generation of an Electronic Signature using a mobile device is considered.

Mobile Signature Service Provider (MSSP): person or entity enabling the generation of Mobile Signatures by Signers and the use of Mobile Signatures by Application Providers

Mobile Signature Service Provider (Roaming MSSP): intermediary body that may provide interoperability between Mobile Signature Service Providers

Personal Identification Number (PIN): number that is used as Signer's Authentication Data

signature attributes: additional information that is signed together with the Signer's Document

Signature Creation Application (SCA): application within the Signature Creation System that creates an electronic signature, excluding the signature creation device

Signature Creation Data (SCD): unique data, such as codes or private cryptographic keys, which are used by the Signer to create an electronic signature

Signature Creation Device (SCD): software or hardware which is used to implement the Signature Creation Data

signature creation environment: physical, geographical and computational environment of the Signature Creation System

signature creation system: overall system that creates an Electronic Signature consisting of the Signature Creation Application and the Signature Creation Device

signature gateway: platform operated by the Mobile Signature Service Provider to enable mobile signature functionality

signature request: message send from the Application Provider to the Mobile Signature Service Provider, requesting a mobile user to create a Mobile Electronic Signature

signature response: message send from the Mobile Signature Service Provider to the Application Provider in response to a Signature Request

Signed Data Object (SDO): this contains the result of the signature process consisting of the Mobile Electronic Signature and possibly the Signer's Document or a hash of it and Signature Attributes with which a Mobile Electronic Signature is associated. It is in the format specified by the selected Signed Data Object Type

Signed Data Object type: type of the Signed Data Object (e.g. as specified in TS 101 733 [20]), which specifies the resultant content and format of the Signed Data Object

signer: person or entity that creates an electronic signature

signer's authentication data: data (e.g. a PIN, password, or biometric data) used to authenticate the Signer to the MSCD and which is required to allow the use of the Signature Creation Data held on the Mobile Signature Creation Device

signer's document: document for which the Signer intends to create a Mobile Signature

signature invocation: non-trivial interaction between the Signer and the Mobile Signature Creation Application or the Mobile Signature Creation Device that is necessary to invoke the start of the signing process (the 'Wilful Act' of the signer)

signature policy: set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid

SIM-Card: smartcard located inside a mobile telephone used to manage the subscriber's access to the mobile telephone network

NOTE: The spare available memory on the SIM-card is often used to provide other services to the subscriber (e.g. telephone address book).

smartcard: card containing a tamper-resistant microprocessor (also called chip-card)

Specialist Task Force (STF): ETSI temporary team of specialist assigned for specific purposes

trusted channel: means by which a security function and a remote trusted IT product can communicate with necessary confidence

trusted path: means by which a user and a security function can communicate with necessary confidence

verifier: entity that verifies an evidence (see ISO/IEC 13888-1 [28])

NOTE: Within the context of the present document this is an entity that validates an Electronic Signature

web service: internet technology

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Application Provider
CA	Certification Authority
CEN	European Committee for Standardization
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CSP	Certification Service Provider
CSPC	CSP interaction Component
CWA	CEN Workshop Agreement
DAC	MSCD/MCSA Communicator
DHC	Data Hashing Component
DTBS	Data To Be Signed
DTBSF	DTBS Formatter/Formatted
DTBSR	DTBS Representation
DTBSV	DTBS Verifier
EAL	Evaluation Assurance Level
EESSI	European Electronic Signature Standardization Initiative.
HTTPS	Hypertext Transfer Protocol Secured
ICCID	Integrated Circuit Card IDentity

NOTE: The unique identifier of a particular subscriber identity module (SIM) card.

LAN	Local Area Network
MSA	Mobile Signature Application
MSCA	Mobile Signature Creation Application
MSCD	Mobile Signature Creation Device
MSCE	Mobile Signature Creation Environment
MSCS	Mobile Signature Creation System
MSE	Mobile Signature Environment
MSSP	Mobile Signature Service Provider
OMA	Open Mobile Alliance
PAC	MSSP/MSCA Communicator
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPC	MSSP/AP Communicator
SAC	Signer Authentication Component
SAD	Signer Authentication Data
SAV	Signature Attribute Viewer
SCC	Signature Creation Component
SCD	Signature Creation Data
SDO	Signer Data Object
SDOC	Signed Data Object Composer
SDP	Signer Document Presentation
SDPC	Signer Document Presentation Component
SIC	Signer Interaction Component
SLC	Signature Logging Component

SMS	Short Message Service
SP	Signature Policy
SSCD	Secure SCD
UAC	User Authentication Component
UMTS	Universal Mobile Telephone System
URI	Uniform Resource Identifier
USB	Universal Serial Bus
WAP	Wireless Application Protocol
WSDL	Web Service Description Language
XAdES	XML Advanced Electronic Signature
XAdES-C	XAdES with Complete validation data
XAdES-T	XAdES with Time-stamp
XML	eXtensible Markup Language

4 Introduction to mobile signature

4.1 Overview

4.1.1 Mobile signature

The following working definition is proposed for the concept of mobile signature:

> *"A universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction"*.

In constructing this definition, the following concepts and ideas were considered:

Universal Method:

- A consistent end user experience.
- The largest interactive community for endusers and application providers.
- An architecture promoting interoperability and lowest deployment costs.
- An architecture offering the lowest transaction costs.

Mobile Device:

- Any device using a mobile network as a communications channel.
- Mobile telephone, PDAs, Laptop-PCs, remote telemetry units.
- Integral (e.g. MNO SIM card) and external (e.g. Dual slot) smartcards.
- With or without smartcards.

Citizen Intention:

- A legitimate transaction instruction.
- Citizen's authorization/permission to proceed with a transaction.
- Engineered in such a way that the citizen cannot have been confused or misled (cf. what you see is what you sign).
- Compliance (or otherwise) with legal effect provisions of EU Directive.

Transaction:

- An interaction requiring the citizen's confirmation in order to proceed, details of which are transmitted to the citizen's mobile device and displayed on the mobile device screen prior to authorization.

4.1.2 Using mobile signature

Mobile signature is a concept that is applicable to all kinds of "applications" and not just those applications which can be accessed through mobile devices. Its use is appropriate for applications requiring a citizen's permission to proceed with completion of a transaction that may be initiated by a voice-call, via interactive voice response systems, via the internet and other electronic communications channels and even face-to-face situations. In this respect, the mobile device may be considered as a 'signing-tool' - the electronic equivalent of a pen.

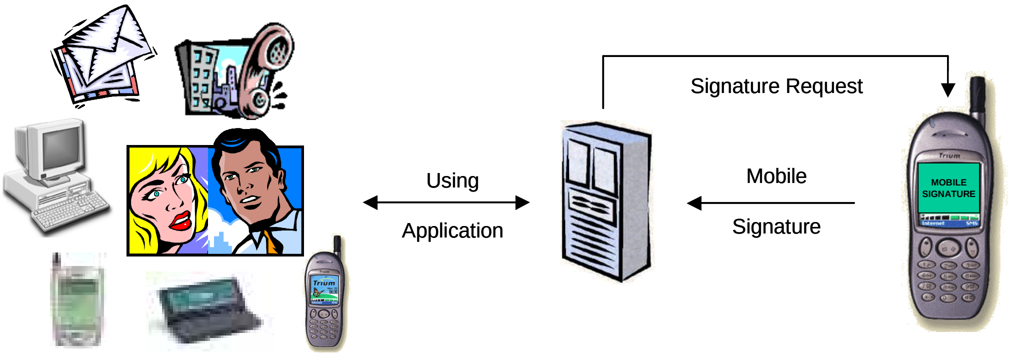


Figure 1: Mobile device as 'Signing Tool' (an electronic pen…)

In considering the use of mobile signature, we consider only the process of forming an electronic signature in relation to a message presented to the citizen. It specifically excludes application level control concerning the signed message. Provision of a mobile signature indicates only that the citizen would like to proceed with a transaction as presented, regardless of whether the citizen is allowed/entitled to do so.

4.1.3 Mobile signature service

Coordination and management of the mobile signature process represents an opportunity to define a MOBILE SIGNATURE SERVICE for citizens and application providers alike. Such an approach might:

- Accelerate adoption of mobile signature by APs (and consequently adoption by Endusers).
- Allow implementation/deployment of a universal API.
- Permit access to an existing base of end-users possessing smartcards and cardreaders.
- Coordinate activation of mobile signature functionality for endusers.
- Coordinate the processing of signature requests for application providers.
- Add value to core mobile signature service (e.g. Timestamp, receipt storage, signature verification etc).
- Leverage existing customer support and communication mechanisms.
- Resolve issues faced by 'traditional' operators of CA platforms (user registration process, legalities, service level agreement).
- Reduce service deployment costs.
- Minimize duplication.
- Aggregate (i.e. acquire) signature traffic.
- Provide a manageable approach to risk reduction.
- Promote interoperability.

A mobile signature service might be provided under the terms of a commercial agreement between a Mobile Signature Service Provider (MSSP) and those parties who choose to rely on mobile signatures for whatever reason. The features of the MSSP role and his/her responsibilities are considered in clause 13 of TR 102 203 [18].

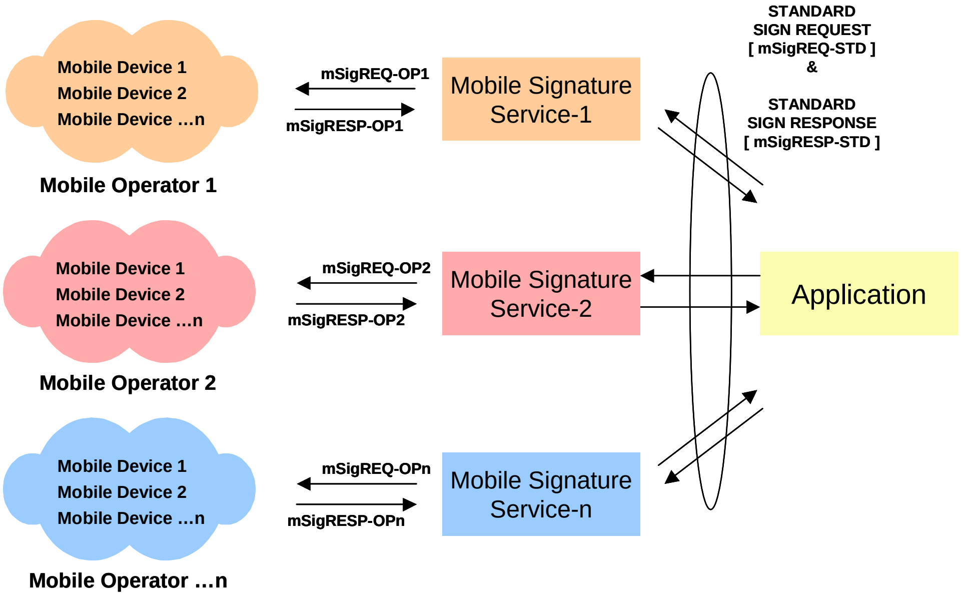


Figure 2: Mobile signature service

A Mobile Signature Service has a standardized interface that may implemented as an Internet Web Service. In this respect, a Mobile Signature Service Provider is an intermediary between endusers and APs that provides and implements a Mobile Signature Web Service.

4.2 Notation

The present document uses schema documents conforming to W3C XML Schema and normative text to describe the syntax and semantics of XML-encoded protocol messages. WSDL

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in the present document are to be interpreted as described in RFC 2119 [15]. When these words are not capitalized, they are meant in their natural-language sense.

4.3 XML Schema declaration

The following XML namespace is used for the Mobile Signature Service:

http://uri.etsi.org/XXXXX/v1.00#

The following namespace declarations apply for the XML schema definitions throughout the present document:

```
<xs:schema
    targetNamespace="http://uri.etsi.org/2000/v1.00#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:mss="http://uri.etsi.org/2000/v1.00#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="qualified"
>
```

This implies that the prefix "ds" is used throughout the document to denote the namespace of the W3C XML-Signature specification according to RFC 3275 [16] while the prefix xs denotes the namespace of the XML-Schema specification [XML-Schema].

The provided XML-Schema is normative.

5 General security analysis

5.1 Architecture

From the general description of the service, we identify three entities:

- the end-user with his mobile signature equipment;
- the Mobile Signature Service Provider (MSSP); and
- the Application Provider (AP).

Security threats can be identified for each entity and security relationships between entities have to be identified as well.

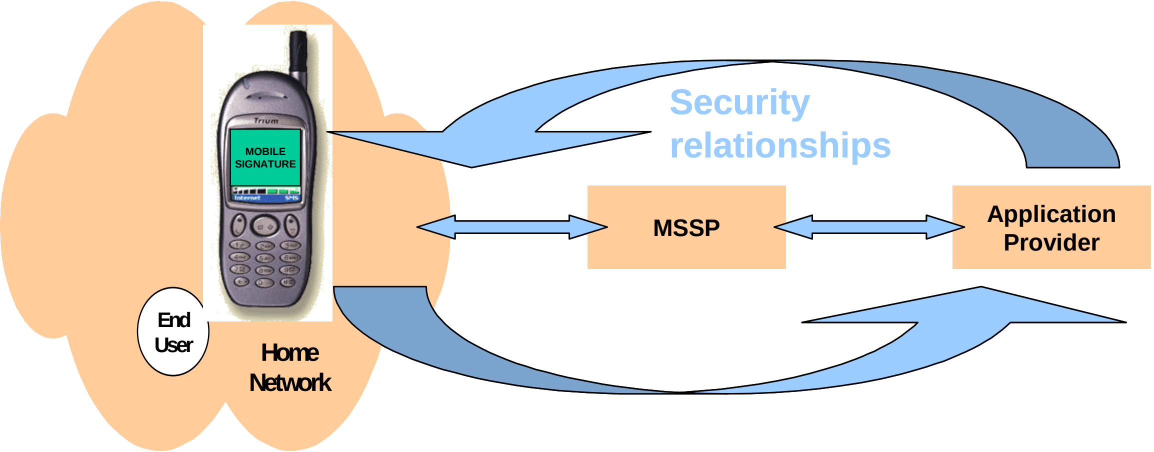


Figure 3: Security analysis of the mobile signature architecture

The reader must recall that the choice of being technology agnostic has been taken in the Business and Functional requirements document (TR 102 203 [18]). Different security features are implemented depending on the mobile equipment (e.g. mobile phone, PDA etc.), the cryptographic technique (e.g. PKI or SKI) and so on. Therefore, while staying technology agnostic, the quality of the Mobile Signature Service may change from one implementation to another according to the security provisioning.

The Application Provider and the end-user must be able to provide and request an appropriate level of security. So, this means that the MSSP must present the AP and the enduser his security capabilities.

In this respect, the present document identifies the relevant security requirements that are specific to the Mobile Signature Service. These requirements are the basis for the specification of common criteria for the description of the mobile signature quality, which will help specifying a graduation of security levels.

5.3 European Directive for electronic signatures

Electronic signatures are defined in article 2 of the EU Directive either as an "electronic signature" or as an "advanced electronic signature":

- Electronic signature:
    - …means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

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

Electronic signatures are further classified by the International Communications and Technology Standards Board (ICTSB) and European Electronic Signature Standardization initiative (EESSI) as:

- Qualified:
    - It is defined as an advanced electronic signature which is based on a qualified certificate and which is created by a Secure Signature Creation Device (see article 2 of the EU Directive). Such electronic signatures are considered as the legal equivalent of a handwritten signature according to article 5.1 of the EU Directive.
- Enhanced:
    - A "qualified" electronic signature with improved protection against certain potential threats as a consequence of applying additional facilities, such as "time-stamping" (i.e. a formal confirmation that the signature was created at a given time).
- General:
    - Any electronic signature that is not a "qualified" electronic signature. Electronic signatures cannot be denied legal effect according to article 5.2 of the EU Directive.

These definitions already represent different security levels for electronic signatures. Therefore, the European standardization activities have in fact identified some kind of **a graduation of the quality of electronic signatures**.

In order, first to improve the understanding of the different types of electronic signatures, and second to facilitate the recognition of the "qualified" electronic signature, EESSI has represented the world of the electronic signature as follows.

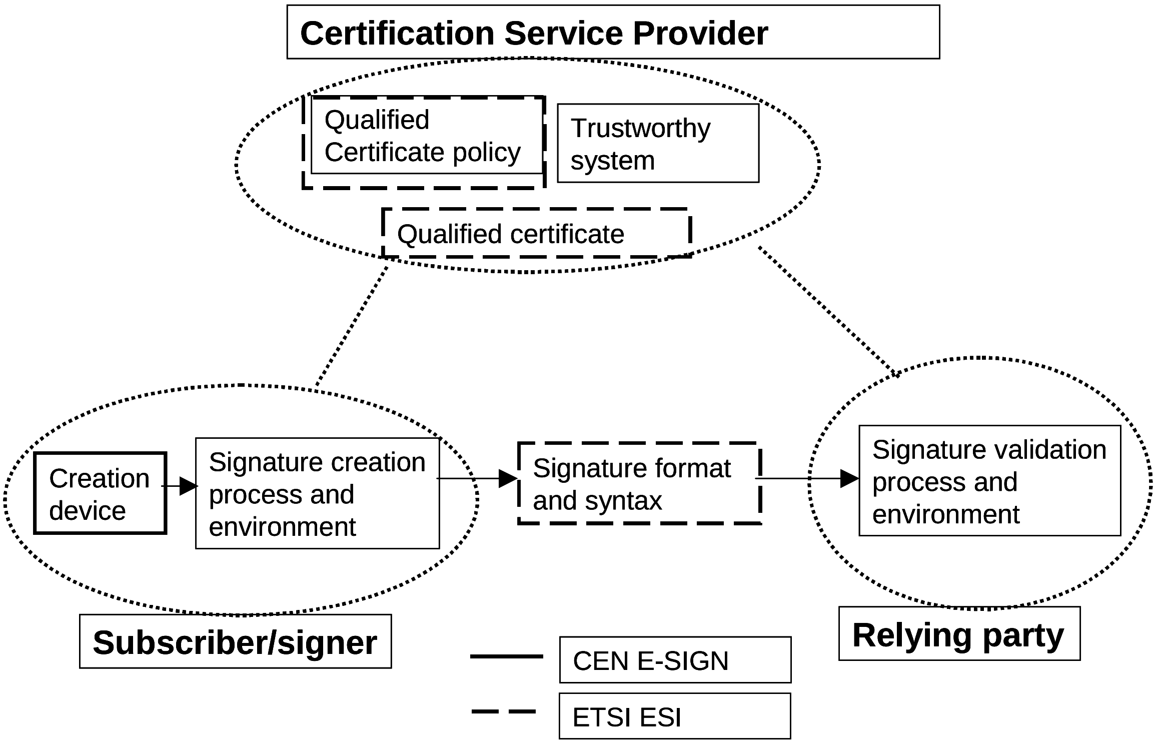

Certification Service Provider
Qualified Certificate policy
Trustworthy system
Qualified certificate
Creation device
Signature creation process and environment
Signature format and syntax
Signature validation process and environment
Subscriber/signer
Relying party
CEN E-SIGN
ETSI ESI

Figure 4: EESSI electronic signature framework

EESSI gathers various standard bodies such as CEN and ETSI in order to work on the different elements of this diagram. The work is distributed among them and it has resulted in the following documents.

ETSI TC Security - ESI WG has been focusing on:

- Signature Policies: TR 102 038 [23], TR 102 041 [24], TR 102 045 [25].
- Qualified certificates: TS 101 456 [19], TS 101 862 [21].
- Electronic Signature Formats: TS 101 733 [20], TS 101 903 [22].

CEN/ISSS E-SIGN Workshop has been focusing on:

- Security requirements for trustworthy systems managing Certificates for Electronic Signatures (CWA 14167-1 [1], CWA 14167-2 [2]).
- Secure Signature Creation devices, version 'EAL 4+' (CWA 14169 [3]).
- Guidelines for the implementation of secure Signature Creation Devices (CWA 14355 [11]).
- Security requirements for Signature Creation Applications (CWA 14170 [4]).
- Procedures for Electronic Signatures verification CWA 14171 [5]).
- EESSI conformance assessment guidance (CWA 14172-1 [6], CWA 14172-2 [7], CWA 14172-3 [8], CWA 14172-4 [9], CWA 14172-5 [10]).

In the diagram above, three major roles are identified: the certification service provider, the relying party and the subscriber/signer. For each role, EESSI defines components of different kind. The security analysis of the overall system corresponds to the security analysis of these components.

All these three roles are relevant in a Mobile Signature Service. However, specific security requirements to the mobile environment are only relevant on the subscriber/signer's side.

The Signer uses a Signature Creation System that is composed of two elements:

- Signature Creation Application:
  - The application within the Signature Creation System that creates an electronic signature, excluding the Signature Creation Device.
- Signature Creation Device:
  - Device which performs all functions using the signer's signature creation data, verifies the signer's authentication data and creates the electronic signature using the signer's signature creation data. Typical Signature Creation Devices are smartcards, USB tokens, PCMCIA tokens etc.

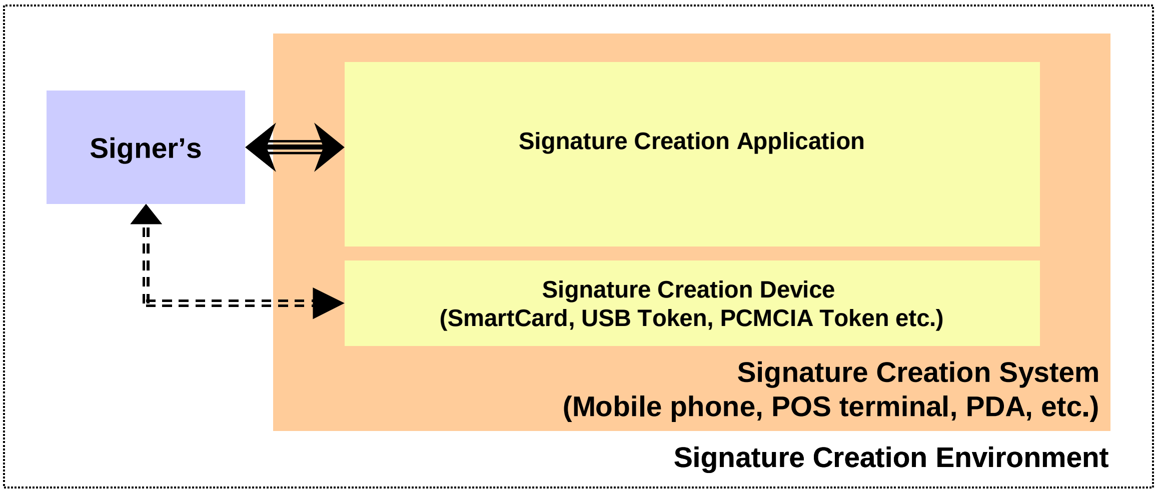

Signer’s
Signature Creation Application
Signature Creation Device
(SmartCard, USB Token, PCMCIA Token etc.)
Signature Creation System
(Mobile phone, POS terminal, PDA, etc.)
Signature Creation Environment

Figure 5: Signature creation environment

A Signature Creation Environment is a physical, geographical and computational environment of a Signature Creation System. EESSI defines security requirements for it, i.e. for Signature Creation Device and the Signature Creation Application. Because of different security environments, those security requirements may be met in different ways. For instance, there are environments were the signer has full control of the Signature Creation System and there are other environments where the Signature Creation Application is under control of a Service Provider.

EESSI mentions in CWA 14170 [4] that a typical Signature Creation Environment, where the individual has full control of the Signature Creation System, is an implementation in a mobile phone. In this case, it is mentioned that "the security requirements may be met by organizational methods by the signer, and the technical means to ensure achievement of the security requirements may be more relaxed".

EESSI defines a minimum set of security requirements that a Signature Creation Device and a Signature Creation Application must meet in order to generate a "qualified" electronic signature. When a Signature Creation Device is compliant with CWA 14169 [3] EAL4+ profile, it is called a Secure Signature Creation Device. Compliance is demonstrated by a formal evaluation process.

For Signature Creation Applications, neither a formal evaluation nor a declaration of conformity is required. However, it is likely that systems, for which a declaration of conformity to the requirements of CWA 14170 [4] is given by the manufacturer, will be regarded as being fundamentally more trustworthy than those from manufacturers who for whatever reason do not make such a declaration (see CWA 14172-4 [9]).

From these security requirements that are identified for all the components involved in the creation of an electronic signature, it is possible to derive different profiles, so that the security level for an electronic signature meets the expectations within a given commercial situation.

So, concerning a Mobile Signature Service, the objectives of the present document are described by the following topics:

- Consistency in respects of the European electronic signature activities
    - How will a mobile signature service be able to provide "qualified" electronic signatures? The requirements defined by EESSI have to match with the requirement for the mobile architecture.
- Specificities of the Mobile Signature Environment
    - Are there additional and specific security requirements for a Mobile Signature Environment? The implementation of the EESSI security requirements in a mobile environment have to be considered.
- Mobile Signature level
    - Are there specific security levels required for Mobile Signatures? Because not all current implementations of Mobile Signature Services are already looking for compliance with the requirements for "qualified" electronic signatures (some may not be able to do it in a short term), specific Mobile Signature Levels may be needed. In this case, the MSSP has to be able to formally describe those levels of security provisioning so that its signature quality may be recognized.

5.3 Identification of a Mobile Signature Environment (MSE)

In order to remain as close as possible with the concepts and methodology of EESSI, we define the following components of a Mobile Signature Creation System.

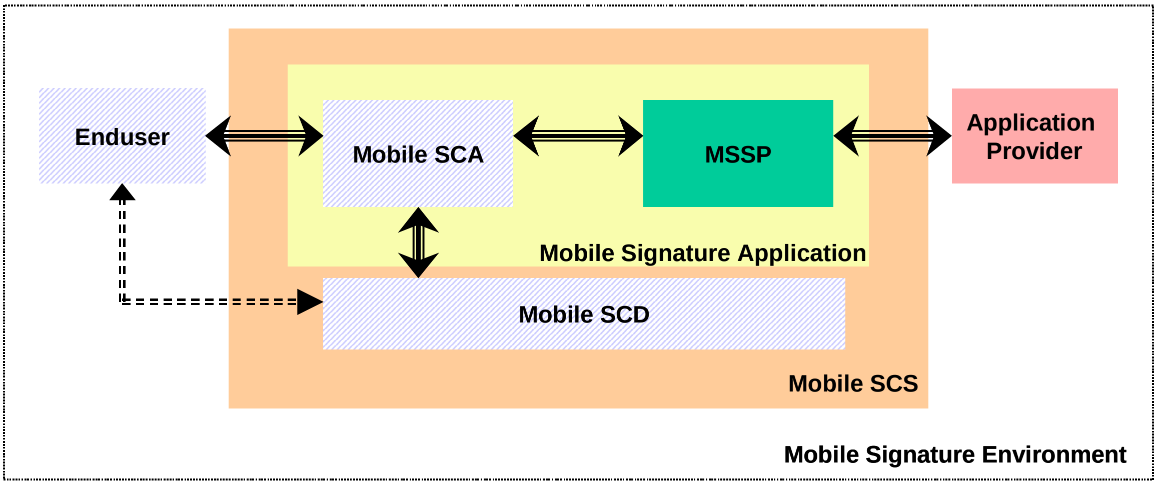


Figure 6: Mobile signature environment

Explanation:

- Enduser: According to the terminology that is used all along the Mobile Signature specifications, the enduser is the Signer.
- Mobile Signature Environment (MSE): The physical, geographical and computational environment of the Mobile Signature Creation System. TR 102 203 [18] describes potential Mobile Signature Environments.
- Mobile Signature Creation System (MSCS): The overall system that creates a Mobile Signature consisting of the Mobile Signature Creation Device and the Mobile Signature Application.
- Mobile Signature Creation Device (MSCD): The equivalent of a Signature Creation Device in a mobile environment. It may be a smart card (e.g. a SIM card).
- Mobile Signature Application (MSA): The mobile application within the MSCS that creates an electronic signature, excluding the MSCD. The MSA consists of the Mobile Signature Creation Application and the Mobile Signature Service Provider.
- Mobile Signature Creation Application (MSCA): Application within the MSCS that creates the Mobile Signature using services from the Mobile Signature Service Provider and the Mobile Signature Creation Device. Within a mobile environment, that's typically a communicating device such as a mobile phone, a communicating PDA etc.
- Mobile Signature Service Provider (MSSP): Provides Mobile Signature Services to the Signer through the MSCA and to the Application Provider.
- Application Provider (AP): A person or entity making use of Mobile Signatures created by Signers. According to the terminology we have used all along the Mobile Signature specifications, the Application Provider is the relying party.

5.4 Operation of the MSA

The Signer, the MSA components, and the MSCD co-operate to create a Mobile Signature in a series of steps. A description of the MSA components involved in this task may be found in clause 6.2 of CWA 14170 [4]. Each of these components is assigned to the MSCA or to the MSSP. However, as the present document is technology agnostic, it does not assume any assignment of the components to the MSCA or the MSSP. For instance, according to the capabilities of a mobile handset, provided that we identify the MSCA with the mobile handset, some components will be more likely implemented by the MSSP on server-side.

Within the diagram below, the components are presented according to a typical realization of a MSA. In this realization, the MSSP supports the MSCA in formatting the message to be signed by the MSCD. However, the formatting could as well be done by the MSCA. On the other hand, all of the tasks performed by components associated to the MSCA may as well be performed by the MSSP.

Figure 7 gives a brief overview of the components assigned to the MSCA and the MSSP.

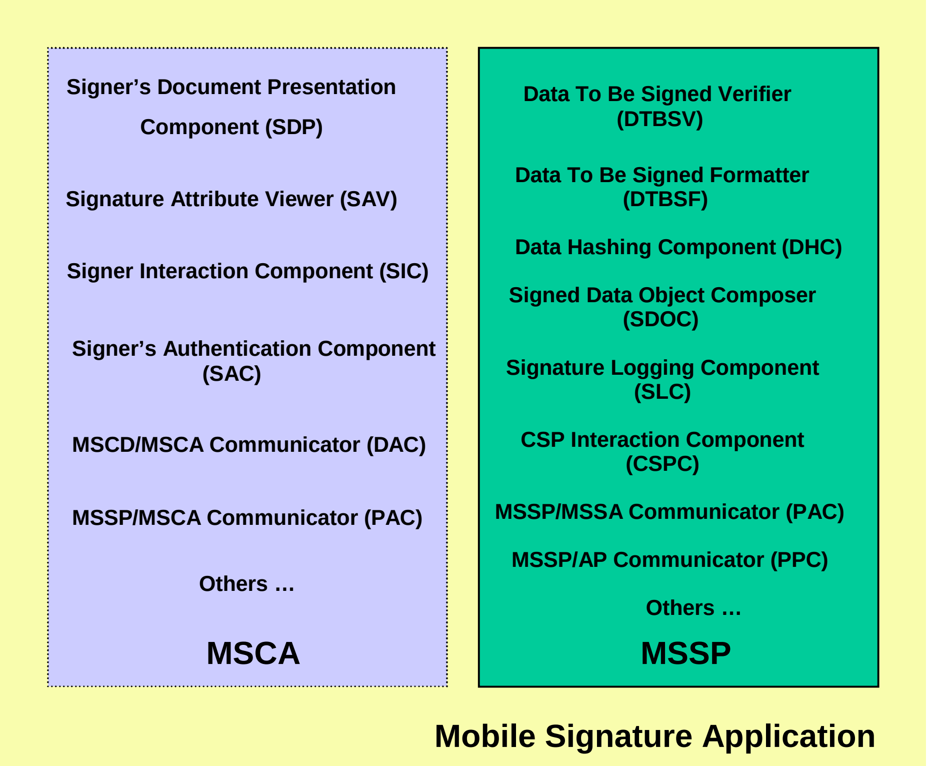

Signer's Document Presentation Component (SDP)
Signature Attribute Viewer (SAV)
Signer Interaction Component (SIC)
Signer's Authentication Component (SAC)
MSCD/MSCA Communicator (DAC)
MSSP/MSCA Communicator (PAC)
Others ...
MSCA
Data To Be Signed Verifier (DTBSV)
Data To Be Signed Formatter (DTBSF)
Data Hashing Component (DHC)
Signed Data Object Composer (SDOC)
Signature Logging Component (SLC)
CSP Interaction Component (CSPC)
MSSP/MSSA Communicator (PAC)
MSSP/AP Communicator (PPC)
Others ...
MSSP
Mobile Signature Application

Figure 7: Inside a mobile signature application...

In order to create a Mobile Signature, the following steps may be carried out, if there are Data To Be Signed (DTBS) sent by the Application Provider to the MSSP (see clause 8 of CWA 14170 [4]).

- The MSSP verifies that the DTBS are syntactically and semantically acceptable. In TS 102 204 [26], what we call DTBS is in fact only the document to be signed. According to the CEN and ESI documents, the DTBS may include the document to be signed, and a signature policy identifier, and a certificate identifier, and a commitment type and others. Anyway, the MSS Signature Request specified in TS 102 204 [26] may contain such additional information. Therefore, the MSSP has the equivalent of the DTBS as defined by the CEN and ESI.

- The MSSP formats the DTBS using the Data To Be Signed Formatter (DTBSF). The result is called Data To Be Signed Formatted (DTBSF). This corresponds for instance to an ASN1 formatting of the DTBS in order to be compliant with PKCS#7 [14].

- The Data Hashing Component (DHC) may then take the DTBSF and compute the DTBS Representation (DTBSR) using the hash process. In some cases all of the hash process is carried out by the MSSP or by the MSCA. In other cases some steps of the hash process may be carried out by the MSCD.

- The DTBSR may then be passed to the MSCA (e.g. a mobile phone) over the MSSP/MSCA Communicator (PAC) on request of the MSCA.

- The MSCA is initialized into its operational mode, if not already done, by starting the MSCA software. The MSCA and the MSSP mutually authenticate each other and the MSSP/MSCA Communicator (PAC) on the MSCA side initiates a trusted channel for the transport of the DTBSR.

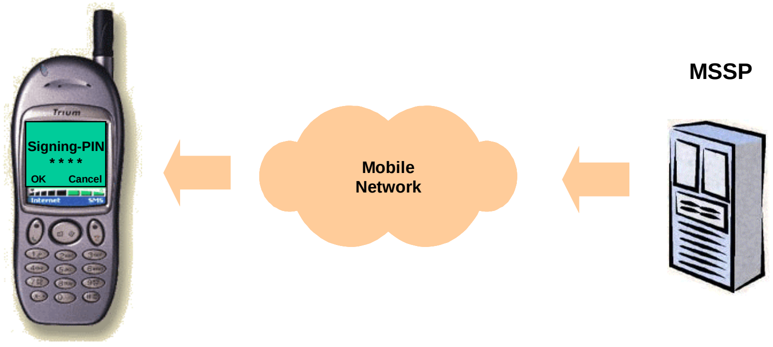
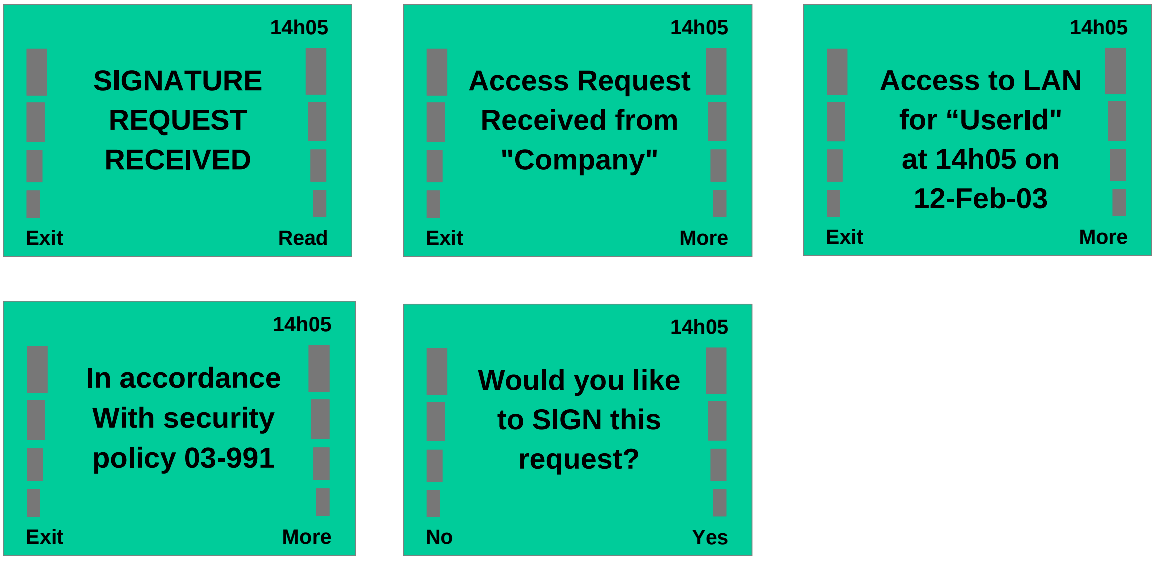


Figure 8: Mobile network: trusted channel for the mobile signature environment

- The MSCA shall allow the Signer to have a view on the DTBSR containing the DTBS and the signature attributes using the Signer's Document Presentation Component (SDPC) and the Signature Attributes Viewer (SAV) to ensure that all of the information in the DTBSR is correct and none is missing.


14h05
SIGNATURE
REQUEST
RECEIVED
Exit Read

14h05
Access Request
Received from
"Company"
Exit More

14h05
Access to LAN
for “UserId"
at 14h05 on
12-Feb-03
Exit More

14h05
In accordance
With security
policy 03-991
Exit More

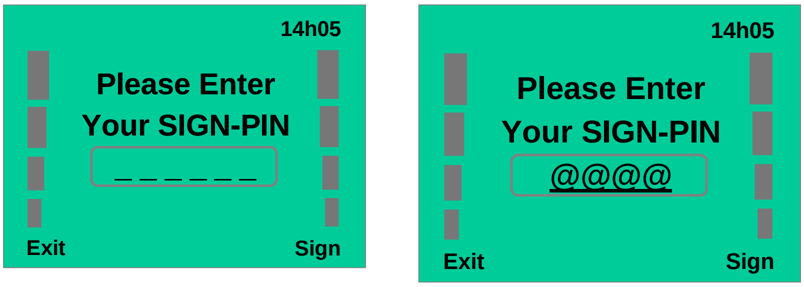
14h05
Would you like
to SIGN this
request?
No Yes

Figure 9: Mobile signature application: screenshot exmaple 1

- The MSCA (e.g. a mobile phone) and the MSCD (e.g. a SIM card) may then mutually authenticate each other, to assure the Signer that the MSCA can be trusted. This mutual authentication is necessary if the MSCA is under control of a service provider, but not if the MSCA is under full control of the Signer.

- The MSCA must than interact with the signer over the Signer Interaction Component (SIC) to obtain a Signature Invocation that instructs the MSCA and the MSCD to initiate the signing process.

- The signer then presents the Signer's Authentication Data (SAD) either to the MSCA or directly to the MSCD (e.g. PIN and/or biometric data) over the Signer Authentication Component (SAC). The SAD is transferred over the MSCD/MSCC Communicator (DAC) providing for a trusted path between these components, if it is not directly input to the MSCD itself.


14h05
Please Enter
Your SIGN-PIN
_ _ _ _ _ _
Exit Sign

14h05
Please Enter
Your SIGN-PIN
@@@@
Exit Sign

Figure 10: Mobile signature application: screenshot exmaple 2

- The DAC may then initiate a trusted channel for the transport of the DTBSR.
- The MSCD then creates the Mobile Signature over the DTBSR using the Signer's Signature Creation Data (SCD).
- The Mobile Signature is then passed back to the MSCA over the DAC and transported to the MSSP.

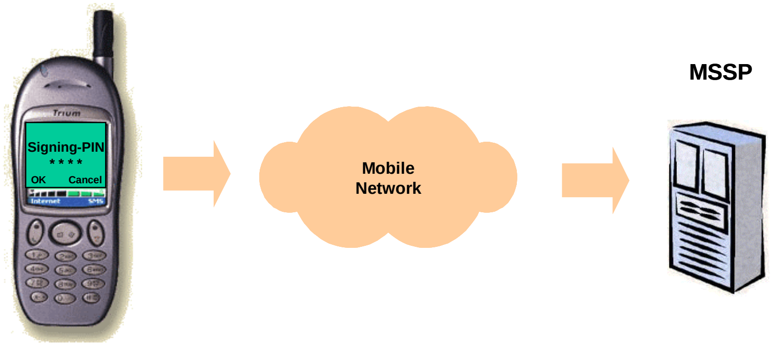
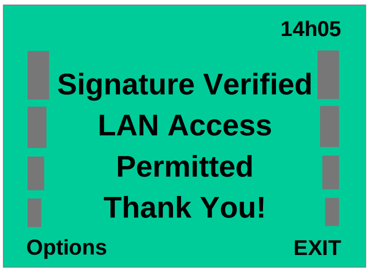


Figure 11: Mobile network: trusted channel for the mobile signature environment

- The Signed Data Object Composer (SDOC) then usually takes the DTBSF components, associates them with the bit string representing the Mobile Signature as delivered by the MSCD, and composes a Signed Data Object (SDO).
- The MSSP imbeds the SDO into the signature response and delivers it to the AP over the MSSP/AP Communicator (PPC). All activities may be logged by the Signature Logging Component (SLC).
- Optionally, if the MSCA or the MSSP is able to verify the signature, it should display the signature verification result.



14h05

Signature Verified
LAN Access
Permitted
Thank You!

Options EXIT

Figure 12: Mobile signature application: screenshot exmaple 3

The detailed minimum security requirements for the Mobile Signature Creation System are described in clause 6.

6 Security requirements for a Mobile Signature Creation System (MSCS)

A general security requirement is that as many security functions as possible should be transferred to secure entities like the MSCD, since they are considered to be more secure and less vulnerable than e.g. the MSCA. However, pragmatic aspects such as efficiency and performance also have to be taken into account, especially in a mobile environment. Therefore, the present document allows for the association of security functions to the MSCA and the MSSP in accordance with the EU Directive.

In the following, the overall security requirements of the MSCS and the security requirements for each of the components of the MSCS (i.e. the MSCA, the MSSP, and the MSCD) are defined.

6.1 Overall security requirements of the MSCS

This clause defines the overall minimum security requirements applicable to each of the components of the MSCS.

6.1.1 Requirements of the DTBS

The DTBS components consist of the Signer's Document and the Signature Attributes. Signature Attributes are pieces of information that support the electronic signature and which are covered by the signature together with the Signer's Document. In particular, the Signer's Certificate, the Signer's Document Content Format, the Signature Policy and the Commitment Type may be required to be part of the DTBS. (A description of the Signature Attributes and its use is contained in TS 101 733 [20].)

The Signer may have a number of different Certificates that are used for different tasks and in different roles. Also, different certificates imply different signature semantics (e.g. contractual signature vs. authentication only). So, there are consequences of accidentally using the wrong Certificate, and the Certificate on which the signature is based shall be indicated in the DTBS.

A Signature Policy reference shall be part of the DTBS if it is needed during the verification process. It may be needed to clarify the precise role and commitments the signer intends to assume with respect to the Signer's Document, and to avoid claims by the verifier that a different Signature Policy was implied by the signer. However, by default the Signature Policy is deemed to be specified in the Signer's Document itself.

A Commitment Type is an indication by the signer of the precise meaning of the signature in the context of the Signature Policy. Its presence in the DTBS will be required whenever a Signature Policy specifies more than a single Commitment Type, each of which may have different legal interpretations of the intent of the signature.

The DTBS shall implicitly or explicitly contain the Signer's Document Content Format that specifies the details of how the document is to be presented or used by the verifier.

All the following requirements of the DTBS face the threat of inappropriate or ambiguous Mobile Signatures.

MSCS1: The DTBS shall contain a Signer's Document.

MSCS2: The DTBS shall contain the Signer's Certificate related to the Signature Creation Data that the MSCD uses to generate the Mobile Signature and intended by the Signer.

MSCS3: The DTBS shall contain the Signature Policy (or a reference to the Signature Policy) for any document that is not considered to implicitly contain a Signature Policy or can be deducted from the context.

MSCS4: The DTBS shall contain the Commitment Type attribute if the Signature Policy defines more than a single Commitment Type.

MSCS5: If the Security Policy in force allows more than one Signer's Document Content Format, the DTBS shall contain the Content Format of the Signer's Document.

6.1.2 Trusted channel requirements

Trusted Channel requirements face the threat of an accidental or malicious corruption of the DTBS components, the DTBSF, the DTBSR, the Mobile Signature, and the SDO whilst they are within the MSCA or MSSP and during transfer between the MSCA and MSSP or between MSCA and MSCD. The Trusted Channel requirements also face the threat of an accidental or malicious breach of confidentiality of the a.m. objects.

MSCS6: The MSCA, MSSP and MSCD shall maintain the integrity of the DTBS components, DTBSF, DTBSR, Mobile Signature, and SDO.

MSCS7: The MSCA, MSSP and MSCD shall maintain the integrity of all protocol data flowing between MSCA and MSSP as well as between MSCA and MSCD.

MSCS8: The MSCA, MSSP and MSCD shall maintain the confidentiality of the DTBS components, DTBSF, DTBSR, Mobile Signature, and SDO.

MSCS9: The System shall ensure that the DTBS components used to create the DTBSF and DTBSR are the same as those presented to the Signer during the representation process and that they are identical to those signed by him.

6.1.3 Requirements resulting from un-trusted processes and communication ports

The following requirements face the threat of interference from un-trusted processes and communication ports within the system.

MSCS10: All un-trusted systems and application processes, peripherals and communication channels shall be prevented from interfering the signing processes.

NOTE: All processes and communication ports which are not required during the signature creation process shall be considered to be un-trusted.

6.1.4 Input control

Input interfaces are always a source of risk since e.g. intruders may try to modify system components or imported viruses may corrupt data and software.

In a mobile environment, it is usual to download applets and plug-ins to enhance the functionality of the mobile device. If trusted system components are imported in such a way, it is necessary that it can be verified that these components come from a trustworthy source and that they are authentic.

The following requirements face the threat of compromised or faked system components.

MSCS11: Provisions shall be made to ensure that viruses are prevented from corrupting MSCS components or that MSCS components that have been subject to a virus attack can be properly reorganized.

MSCS12: The MSCS components shall protect the integrity of its functional components and avoid the possibility that intruders can corrupt them.

MSCS13: Provisions shall be made in the MSCS components that imported components are only installed using a secure download.

6.2 Mobile Signature Creation Application (MSCA)

This clause defines the overall minimum security requirements applicable to each of the components of the MSCA.

6.2.1 Signer's Document Presentation component (SDP)

The SDP component shall securely present the Signer's Document to the Signer. In order to do so, each Signer's Document shall implicitly or explicitly contain a Content Format that specifies the details of how the document is to be presented or used by the verifier. The SDP shall be capable of presenting the document in a Content Format that the SDP fully supports. It shall warn the Signer, if this is not the case.

In practice, a SDP in a mobile environment is only able to support a very limited number of Content Formats and the conditions may easily be met if always the same Content Format is used within the System. This will also limit the Signer's Document complexity. For instance, this may be achieved by using only a declared ASCII characters set.

The following requirements face the threat of signing a document that the signer does not intend to sign.

MSCA1: The SDP shall warn the signer if the Signer's Document does not conform to the syntax specified by the Content Format and allow the Signer to abort from the signature process.

MSCA2: The SDP shall warn the Signer if the Content Format indicated by the Signer's Document is not fully supported by the SDP or otherwise be unacceptable for the SDP and allow the Signer to abort from the signature process.

MSCA3: The SDP shall inform the Signer that other SDOs are embedded in the Signer's Document (this shall prohibit the signer from un-knowingly signing objects with false or otherwise non-valid signatures created by others).

MSCA4: The SDP shall not allow the Signer to change any part of the Signer's Document.

MSCA5: The SDP shall warn the Signer of the presence of hidden text, macros or active code and allow the Signer to abort from the signature process.

6.2.2 Signature Attribute Viewer (SAV)

Signature Attributes are pieces of information that support the electronic signature and which are covered by the signature together with the Signer's Document (as described in clause 6.1.1).

The SAV should allow the signer to examine all Signature Attributes. In particular, the signer needs to be able to check the content of the Signer's Certificate, the Signer's Document Content Format (if present), the Signature Policy (if present) and the Commitment Type (if present).

The following requirements face the threat of signing a document including attributes that the Signer does not intend to include.

MSCA6: The Signature Attribute presentation process shall allow the Signer to view the Signature Attributes.

MSCA7: The attribute viewer process shall warn the Signer of the presence of any hidden or active components (word processor macros etc.) that are embedded in the Signature Attributes.

MSCA8: The SAV component shall allow the signer to inspect the major components of the certificate included in the DTBS.

6.2.3 Signer Interaction Component (SIC)

Prior to creating a Mobile Signature, the MSCA must determine that the signer really wants to create a signature and this cannot come about by accident. This is called a "wilful act" in the EU Directive and "Signature Invocation" in the present document.

A Signature Invocation is a signal from the Signer to the MSCA over the SIC component indicating that the Signer is satisfied that the MSCA is referencing the correct Signer's Document and the correct Signature Attributes as verified by the presentation process, and the Signer wishes to create a Mobile Signature covering them.

After Signature Invocation, the signer then presents the Signer's Authentication Data (SAD). It is necessary to prevent situations in which the Signer remains inactive after the presentation of the SAD because the Signer may be detracted from signature processing and another unauthorized person might possibly be able to complete the signature process.

The following requirements face the threat of unwillingly created signatures.

MSCA9: Prior to initiation of the signature process, the SIC shall request the Signer to perform a non-trivial Signature Invocation interaction with the SCA that is unlikely to occur accidentally.

MSCA10: The SIC shall place a limit on the time that elapses between provision of the SAD and completion of the Signature Invocation.

MSCA11: If this time limit lapses, then the whole signature process shall be terminated and the Signer shall be required to restart the signature process from re-inputting the SAD.

6.2.4 Signer's Authentication Component (SAC)

Before creating a Mobile Signature, the MSCD must be sure that the signer is the owner of (or is authorized to use) the MSCD. It does this by obtaining the Signer's Authentication Data (SAD) from the signer. In some MSCA/MSCD configurations, the SAD is passed from the signer through the MSCA, and then transferred to the MSCD. In this case the requirements stated in this clause are addressed to the MSCA, otherwise they are addressed to the MSCD.

Before the SAD may be passed to the MSCD, a Trusted Path has to be established. The Trusted Path provides confidence that the Signer is communicating directly with the MSCD whenever it is invoked. Untrusted applications cannot intercept or modify the input of the Signer.

The following requirements face the threat of an unauthorized use of the MSCD.

MSCA12: The MSCA shall provide a means for the Signer to input SAD through to MSCA to the MSCD.

MSCA13: The MSCA shall maintain confidentiality of the SAD and securely erase it as soon as it is no longer needed.

MSCA14: If the wrong SAD is repeatedly provided (e.g. on three successive occasions), an error response to the signer shall be generated and a retry permitted if the signer's authentication method has not been blocked by the MSCA.

MSCA15: A Trusted Path for the transaction of SAD to the SSCD shall be provided through the MSCA.

MSCA16: A function for changing a knowledge based SAD shall be provided, unless the use of this function is forbidden by security policy.

MSCA17: The presented SAD shall not be displayed, but a feedback shall be provided by a method that does not reveal the SAD.

MSCA18: The MSCA shall require the representation of a new SAD twice and check whether both presentations are identical before delivering the new SAD to the MSCD.

6.2.5 MSCD/MSCA Communicator (DAC)

The DAC component performs all the necessary interactions between MSCA and MSCD. Therefore, from the viewpoint of security, it is a very sensitive component, because any malfunction may result in the creation of a wrong signature.

The MSCD functionality may be implemented on a platform (e.g. on a smartcard) which carries one or more MSCD functions (often referred as "Applications"). If such a multi-application platform is used as the carrier of one or more logical MCSDs, then the MCSA has to select one of them (e.g. by using the associated application identifier).

If the MSCD holds more than one instance of Signature Creation Data, then the appropriate one has to be selected. Even if the MSCD has only one single Signature Creation Data, the MSCD may require that a reference to it is set.

The following requirements face the threat of producing wrong signatures by the MSCD.

MSCA19: The DAC component shall support all items relevant to the physical interface in the intended range or with its specified characteristics to ensure proper operation of the types of MSCDs that it claims to support.

MSCA20: The DAC component shall ensure that the correct MSCD functionality is selected, if the platform, on which the MSCD functionality is implemented, requires a selection.

6.2.6 MSSP/MSCA Communicator (PAC)

The PAC performs all the necessary interactions between the MSSP and the MSCA, i.e. the transport of the DTBSF and the return of the Mobile Signature.

Some of the security requirements addressed to this component are already covered in clause 6.1.2: Confidentiality and integrity of the data exchanged between the MSSP and the MSCA.

MSCA21: The MSCA (e.g. a mobile phone) and the MSSP shall mutually authenticate each other, to assure the Signer that the MSSP and this particular Mobile Signature request can be trusted.

6.3 Mobile Signature Service Provider (MSSP)

This clause defines the overall minimum security requirements applicable to each of the components of the MSSP.

6.3.1 Data To Be Signed Verifier (DTBSV)

This function is used for the extraction of the DTBS from the Signature Request message sent from the AP and the verification of the DTBS components. The verification of the DTBS should also be performed by the Signer using the SDP and SAV components. However, as the Signer's Document is not generated by the Signer itself but by the AP, an additional verification by the MSSP in support of the Signer is required because of the additional threats the Signer faces in this situation.

The DTBSV is a component not foreseen in CWA 14170 [4] because of a different situation. In CWA 14170 [4] is it assumed that the Signer himself creates the DTBS and uses the SDP and SAV components for a verification of the DTBS. In the present document, it is assumed that the DTBS is not created by the Signer but the AP. The DTBS creation process is completely out of Signer's control. He is only able to verify the results. This situation is prone to additional threats compared to the situation which is assumed in CWA 14170 [4].

The Signer might not always fully understand the implications of the Signature Attributes part of the DTBS generated by the AP (as described in clause 6.1.1). He might for instance not be aware of signing a document that becomes legally binding. The Signer may also not be aware of any ambiguity within the DTBS that could have been thoroughly placed by a perfidious AP.

Therefore, the Signer has to be protected against such threats by the MSSP which shall inform the Signer about the possibly harmful implications of signing the document. On the other hand, the warning from the MSSP might annoy a signer already exactly knowing the consequences of his signature. It may be difficult to find out, which warnings are appropriate in each case.

In addition to that, it is not easy for the MSSP to deal with problems found during the verification of the DTBS. As described in clause 6.2.1, problems may for instance result from an ambiguity of the Signer's Document because through lack of Content Format information or inadequate Signer's Document presentation due to SDP limitations.

There are, however, two conflicting arguments that the MSSP has to take into account in this case. On one hand, the MSSP shall protect the Signer against threats resulting from ambiguous signatures. On the other hand, the MSSP shall leave the decision to the Signer whether he wants to bear those risks.

Therefore, the MSSP must not reject any Signature Request if there are any problems discovered during verification. In most cases, a warning of the Signer should be sufficient. However, if the MSSP rejects a Signature Request from an AP, the Signer shall be informed by the MSSP that there was a Signature Request from an AP and indicate the reasons for its rejection.

In any case, the MSSP must not change an DTBS from an AP without his consent. The MSSP could for instance include an appropriate Signer's Document Content Format in order to avoid mis-interpretations of the Signer's Document through lack of Content Format information. The AP, however, might have its own interpretation of the DTBS and might not become aware the interpretation of the Signer's Document is now clear because of that change, but different.

The following requirements face the threats of the Signer and the AP regarding inappropriate Content Formats and Signature Attributes.

MSSP1: The MSSP shall verify all the DTBS components extracted from the Signature Request according to the requirements MSCA1, MSCA2, MSCA3, MSCA5, and MSCA7.

MSSP2: The MSSP shall warn the Signer generating a warning as described in clause 6.2.1.

MSSP3: The MSSP shall inform the Signer about the implications of the Signer's Document, if necessary.

MSSP4: The MSSP shall reject the Signature Request if necessary.

MSSP5: The MSSP must not change an DTBS from an AP without its consent.

6.3.2 Data To Be Signed Formatter (DTBSF)

The DTBSF component takes the Signer's Document and the signature attributes from the Signature Request of the AP and formats it. If the DTBS is to contain a hash value of the Signer's Document, and this does not already exist, then the DTBSF component initiates the hashing before producing the DTBSF.

In some MSCA/MSSP configurations, the formatting of the DTBS is done by the MSCA component. In this case the requirements stated in this clause are addressed to the MSCA.

The following requirements face the threat of a wrong or incomplete DTBS production.

MSSP6: The MSSP shall produce the DTBSF format as indicated by the Signature Request.

6.3.3 Data Hashing Component (DHC)

The DHC component takes the DTBSF and produces the DTBSR. The DTBSR is the result of a hash function applied to the DTBSF and a formatting of the hash value, also referred to as padding, if required by the signature algorithm, e.g. PKCS#1 [13].

In some configurations, the hashing may be performed by the MSCA or the MSCD. There are also configurations where the MSCD performs a partial hashing, i.e. hashing of last rounds on the MSCD. However, at least complete hashing in an MSCD is only feasible if the MSCD has a high-speed interface like USB. For a MSCD of the smartcard type, this configuration may not be appropriate.

The following requirements face the threat of using weak algorithms and an incomplete DTBSR.

MSSP7: The MSSP shall insure that only those hash algorithms are used that belong to a set of approved algorithms and parameters for Mobile Signatures (see SR 002 176 [17]).

MSSP8: The MSSP shall insure that only those electronic signature input formats are used that are allowed by the set of approved algorithms and parameters for Mobile Signatures.

MSSP9: The MSSP shall ensure the production of the correct DTBSR for a Mobile Signature.

6.3.4 Signed Data Object Composer (SDOC)

The SDOC associates the output of the MSCD (the Mobile Signature) which the DTBSF according to the standard format determined by SDO Type and creates the Signed Data Object (SDO).

There are no security requirements addressed to the SDOC. However, it is essential that the resulting SDO has the same structure as the DTBS, e.g. the sequencing of the Signer's Document and the Signature Attributes is the same. Otherwise, the Mobile Signature will not be valid.

6.3.5 CSP Interaction Component (CSPC)

The CSPC interacts with Certification Service Providers (CSP) in order to import Signer's Certificates and check their status.

There are no security requirements addressed to the CSPC. However, it is advisable to make regular checks on the validity of the Signer's Certificates.

6.3.6 Signature Logging Component (SLC)

For the Signer, it is useful to get support from the MSSP with respect to signature logging, i.e. for each created signature, a logging record may be stored by the MSSP.

Obviously, a written log record shall not be modified. Apart of that, there are no specific security requirements addressed to the SLC. However, it is recommended that a count of the number of signatures should be maintained.

6.3.7 MSSP/MSCA Communicator (PAC)

The PAC component takes the DTBSR produced by the DHC Component, and sends it to the MSCA for a representation to the Signer. The PAC shall add all warnings generated by the DTBSV.

The PAC performs all the necessary interactions between the MSSP and the MSCA, i.e. the transport of the DTBSF and the return of the Mobile Signature.

Some of the security requirements addressed to this component are already covered in clause 6.1.2: Confidentiality and integrity of the data exchanged between the MSSP and the MSCA.

MSSP10: The MSCA (e.g. a mobile phone) and the MSSP shall mutually authenticate each other, to assure the Signer that the MSSP and this particular Mobile Signature request can be trusted.

6.3.8 MSSP/AP Communicator (MAC)

The MAC performs all the necessary interactions between the MSSP and the AP, i.e. the transport of the Signature Request and the Signature Response.

Some of the security requirements addressed to this component are already covered in clause 6.1.2: Confidentiality and integrity of the data exchanged between the MSSP and the AP.

MSSP11: The AP and the MSSP shall mutually authenticate each other.

6.4 Mobile Signature Creation Device (MSCD)

The MSCD is composed of components related to signature creation, user authentication, personalization, and either SCD/SVD generation with SVD export or SCD import, if that data is generated externally. Within the present document, the security requirements for the Signature Creation Component and the User Authentication Component are identified.

For all data exchange with the MSCD, a trusted path is required according to clause 6.1.2 describing the overall security requirements for the MSCS. There are also overall security requirements for the MSCD Components.

6.4.1 Overall security requirements for the MSCD

The overall security requirements for the MSCD are related to self testing of the MSCD Components, emanation security, prevention of a secure state, and detection of physical attacks.

Self testing is required in order to demonstrate the correct operation of the MSCD components. The self tests shall be performed during the initial start-up process, and may be performed during normal operation or at request of an authorized user.

The MSCD shall prevent attacks against the Signer's Authentication Data (SAD) and the Signature Creation Data (SCD) where the attack is based on external observable physical phenomena, e.g. power consumption, timing of transitions to internal states, electromagnetic radiation, and radio emission. Such phenomena may origin from a data exchange via one of the interfaces or from internal operation. The set of measurable physical phenomena is influenced by the technology employed for the implementation of the MSCD.

The following requirements are related to all MSCD components.

MSCD1: The MSCD shall run a suite of tests to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the security functions.

MSCD2: The MSCD shall run a suite of tests to demonstrate the correct operation of the security functions.

MSCD3: The MSCD shall provide authorized users with the capability to verify the integrity of security functions data.

MSCD4: The MSCD shall provide authorized users with the capability to verify the integrity of stored executable code of the security functions.

MSCD5: The MSCD shall not emit data in excess so that attackers are not able to gain access to SAD or SCD.

MSCD6: The MSCD shall ensure that attackers are unable to use the interfaces to gain access to SAD or SCD.

MSCD7: The MSCD shall preserve a secure state when security relevant failures occur.

MSCD8: The MSCD shall provide unambiguous detection of physical tampering that might compromise the security functions.

MSCD9: The MSCD shall provide the capability to determine whether physical tampering has occurred.

MSCD10: The MSCD shall resist tampering by responding automatically such that the security is not violated.

6.4.2 User Authentication Component (UAC)

The Signer must be authenticated to create signatures. Therefore, the SAD are sent to the MSCD. The MSCD may have a Human Interface (HI) for the input of the Authentication Data. Otherwise, a HI at the MSCA and a Trusted Path between the MSCA and the MSCD has to be provided (see clause 6.2.4).

If the MSCD has a HI, the following requirements from clause 6.2.4, facing the threat of an unauthorized use of the MSCD, have to be met.

MSCD11: The MSCD shall provide a HI for the input of the SAD.

MSCD12: The MSCD shall maintain confidentiality of the SAD and securely erase it as soon as it is no longer needed.

MSCD13: If the wrong SAD is repeatedly provided (e.g. on three successive occasions), an error response to the signer shall be generated and a retry permitted if the signer's authentication method has not been blocked by the MSCD.

MSCD14: A function for changing a knowledge based SAD shall be provided, unless the use of this function is forbidden by security policy.

MSCD15: The presented SAD shall not be displayed, but a feedback shall be provided by a method that does not reveal the SAD.

MSCD16: The MSCD shall require the representation of a new SAD twice and check whether both presentations are identical.

6.4.3 Signature Creation Component (SCC)

If the Signer is authenticated, the Data To Be Signed Representation (DTBSR), i.e. the DTBSF itself, a hash value of the DTBSF, or a pre-hashed value of the DTBSF, may be transferred to the MSCD over a Trusted Channel, if required. The SCC than performs the signature creation and the hashing, if required. As the result, the Mobile Signature is returned (over that channel).

The following requirements face the threats of using inappropriate algorithms and of unauthorized generation of electronic signatures.

MSCD17: The SCC shall require the Signer to be successfully authenticated before allowing signature creation or any other actions on behalf of that user.

MSCD18: The SCC shall ensure that only an user in the role of the Signer is able to sign the DTBSR.

MSCD19: The SCC shall perform signature creation in accordance with specified cryptographic algorithms and cryptographic key length that belong to a set of approved algorithms and parameters (see SR 002 176 [17]).

MSCD20: The SCC shall be able to destroy the SCD on demand of the Signer or the administrator in accordance with a specified key destruction method.

7 Mobile signature profile

7.1 Rationales

As described in clause 6 of the present document, there may be different implementations of a Mobile Signature Service providing for the same level of security. From a security viewpoint it may not be the most important question, to which of the system components the security functions are associated. More important is the question, if all the security functions identified in clause 6 are foreseen. Furthermore, the quality of the implementation of the security functions may be a concern.

Apart from the MSCS itself, the environment of the system and operational aspects have to be taken into account. Part of the environment is the CSP that provides the Signer with certificates, status information, timestamps, etc. Lack of quality of the CSP functions may result in a diminished quality of the Mobile Signature. This also may result from disregarding organizational security policies by the personal of CSPs that have got no accreditation.

If environmental topics are taken into account, the following broad categories of Mobile Signatures may be identified according to the EU Directive (see clause 5.3):

- simple electronic signature (article 5.2);
- advanced electronic signature (article 2.2);
- advanced electronic signature + qualified certificate;
- advanced electronic signature + simple certificate + SCD (or SSCD);
- advanced electronic signature + qualified certificate + SCD;
- "qualified" electronic signature (article 5.1);
- "qualified" electronic signature + CSP accreditation.
- ...

The categories of the Mobile Signatures are roughly ordered according to an ascending security level. In comparing two instances of Mobil Signatures, it is not always clear which one has the higher level. Therefore, it is not possible to define a linear order for Mobile Signatures. This makes it even more difficult to identify appropriate levels.

However, within a closed environment where all the actors have commercial agreements between each others, a set of rules may be defined so that a proprietary ranking of different Mobile Signatures Profiles is available. A closed environment may be one MSSP and its acquired Service Provider, or a Mobile signature Mesh (see TS 102 207 [27]) and its acquired Service Providers.

7.2 Framework

Given the security analysis we have made in clause 6 and the rationales above, we can conclude that even if it is be difficult to define an objective standard for the ranking of Mobile Signature Profiles, it is possible to define a useful framework for Mobile Signature Profiles.

Below is given a list of information that should be part of the framework for Mobile Signature Profile:

- Registration and certification:
  - Registration: face to face or distant, level of credentials, definition of Identity.
  - Certification: Certificate Practice Statement, Certificate Policy, management and use of Identity.

- Mobile Signature System:
    - Rules for the Mobile Signature Processing:
        - Signature Policy see TR 102 038 [23], TR 102 041 [24], TR 102 045 [25].
          Signature Policies are an adequate means for the provision of notice about the signature quality. A relying party needs to be sure that the policy invoked by the Signer is appropriate for his specific business needs. The signer is requested "to provide notice of the signing conditions that apply on each transaction with its business counterpart" (clause 7.1 of TR 102 041 [24]). Signature Policies shall contain management practices of the signing conditions and technical rules, e.g.:
            - management and use of identity and attribute certificates;
            - qualified/non-qualified certificates;
            - signature creation procedures;
            - algorithms/key length.
    - Mobile Signature Technical Protection:
        - Overall Security Requirements.
        - Mobile SCA:
            - Accreditation or voluntary declaration of conformity with a formal profile provided as a URI.
            - Technical Components (requirements for each):
                - Signer's Document Presentation.
                - Signature Attribute Viewer.
                - Signer Interaction.
                - Signer's Authentication.
                - MSCD/MSCA Communicator.
                - MSSP/MSCA Communicator.
        - MSSP:
            - Accreditation or voluntary declaration of conformity with a formal profile provided as a URI.
            - Technical Components (requirements for each):
                - Data To Be Signed Verifier.
                - Data To Be Signed Formatter.
                - Data Hashing.
                - Signed Data Object Composer.
                - Signature Logging Component.
                - CSP Interaction.
                - MSSP/MSCA Communicator.
                - MSSP/AP Communicator.

- Mobile SCD:
    - Accreditation or voluntary declaration of conformity with a formal profile provided as a URI.
    - Technical Components (requirements for each):
        - User Authentication.
        - Signature Creation.
        - MSCD/MSCA Communicator.

Some of this information is already specified or being specified by other standardization bodies, such as ESI for Signature Policies.

7.3 XML Schema

Like a XML schema defined by ESI for signature policy, a XML Schema for a Mobile Signature Profile framework may be defined. In the present document, we only focus on the technical protection part of Mobile Signature Profile. In this respect, we propose to use the following XML schema:

```
<xs:schema
    targetNamespace="http://uri.etsi.org/2000/v1.00#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:mss="http://uri.etsi.org/2000/v1.00#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="qualified"
>

    <xs:complexType name="technicalComponent_Type">
    <annotation>
    This is a generic description of the protection features of a technical component.
    </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="MSCA_Type">
    <annotation>
    This is a generic description of the protection features of a Mobile Signature Creation
Application.
   SDP : Signer's Document Presentation
   SAV : Signature Attribute Viewer
   SIC : Signer Interaction
   SAC : Signer's Authentication
   DAC : MSCD/MSCA Communicator
   PAC : MSSP/MSCA Communicator
An example of a voluntary declaration of conformity for Signature Creation Applications can be found
in CEN CWA 14172-4
    </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:element name="SDP" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="SAV" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="SIC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="SAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="DAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="PAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="MSSP_Type">
    <annotation>
    This is a generic description of the protection features of a Mobile Signature Service Provider.
   DTBSV : Data to Be Signed Verifier
   DTBSF : Data To Be Signed Formatter
   DHC : Data Hashing Component
   SDOC : Signed Data Object Composer
   SLC : Signature Logging Component
   CSPC : CSP Interaction Component
     PAC : MSSP/MSCA Communicator
     PPC: MSSP/AP Communicator
    </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:element name="DTBSV" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="DTBSF" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="DHC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="PPC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="PAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="MSCD_Type">
    <annotation>
    This is a generic description of the protection features of a Mobile Signature Creation Device.
  </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:element name="userAuthentication" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="signatureCreation" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="technicalProtection_Type">
    <annotation>
    This is a generic description of a Mobile Signature Service Technical Protection. This structure
denotes the security analysis of clause 6. MSCS elememt denotes the overall security requirements
for a MSCS. MSCA, MSSP and MSCD are used to go further in the description of the security features
of a MSCS.
</annotation>
                <xs:sequence>
                    <xs:element name="MSCA" type="mss:MSCA_Type"/>
                    <xs:element name="MSSP" type="mss:MSSP_Type"/>
                    <xs:element name="MSCD" type="mss:MSCD_Type"/>
                    <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:element name="MSS_Profile" type="mss:ProfileType"/>
    <annotation>
    This is a generic description of a Mobile Signature Profile. As we focus only on the technical
protection aspect, this is the only element we mention. However, extensions can be added thanks to
the "any" element.
</annotation>
    <xs:complexType name="ProfileType">
                <xs:sequence>
                    <xs:element name="MSS_technicalProtection" type="mss:technicalProtection_Type"/>
                    <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
    </xs:complexType
```

7.3.1 URIs

For each technical component, the following URIs denote the corresponding security requirements.

7.3.1.1 MSCS

http://uri.etsi.org/TS102206/v1.1.3#MSCS: Requirements MSCS 1 → 13

7.3.1.2 MSCA

http://uri.etsi.org/TS102206/v1.1.3#SDP: Requirements MSCA 1 → 5

http://uri.etsi.org/TS102206/v1.1.3#SAV: Requirements MSCA 6 → 8

http://uri.etsi.org/TS102206/v1.1.3#SIC: Requirement MSCA 9 → 11

http://uri.etsi.org/TS102206/v1.1.3#SAC: Requirement MSCA 12 → 18

http://uri.etsi.org/TS102206/v1.1.3#DAC: Requirement MSCA 19 → 20

http://uri.etsi.org/TS102206/v1.1.3#PAC: Requirement MSCA 21

7.3.1.3 MSSP

http://uri.etsi.org/TS102206/v1.1.3#DTBSV: Requirement MSSP 1 → 5

http://uri.etsi.org/TS102206/v1.1.3#DTBSF: Requirement MSSP 6

http://uri.etsi.org/TS102206/v1.1.3#DHC: Requirement MSSP 7 → 9

http://uri.etsi.org/TS102206/v1.1.3#PAC: Requirement MSSP 10

http://uri.etsi.org/TS102206/v1.1.3#PPC: Requirement MSSP 11

7.3.1.4 MSCD

http://uri.etsi.org/TS102206/v1.1.3#MSCD: Requirement MSCD 1 → 10

http://uri.etsi.org/TS102206/v1.1.3#UserAuthentication: Requirement MSCD 11 → 16

http://uri.etsi.org/TS102206/v1.1.3#SignatureCreation: Requirement MSCD 17 → 20

7.3.2 Example 1

Here is the description of a classical Mobile Signature Service as it may be deployed in the real world:

SCD → SIM Card with SIM toolkit application using PKI algorithm. Accreditation ISO EAL 4+ according to the Protection Profile specified by CEN CWA 14169 [3] for Secure Signature Creation Device type 3.

MSSP → Platform that has no real problems to develop all the security features described in clause 6.

SCA → Mobile phone that is SIM toolkit compliant.

Communication between SCA and MSSP is performed by SMS with TS 101 181 [29] (GSM 03.48) security features: Encryption, Checksum and redundancy control.

Communication between MSSP and AP is performed by HTTP with SSL security features.

```
<MSS_Profile>
    <MSS_technicalProtection>
        <MSCA>
            <PAC Profile=http://uri.etsi.org/TS102206/v1.1.3#PAC />
        </MSCA>
    <MSSP>
            <DTBS Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSV />
            <DTBSF Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSF />
            <DHC Profile=http://uri.etsi.org/TS102206/v1.1.3#DHC />
            <PPC Profile=http://uri.etsi.org/TS102206/v1.1.3#PPC />
        <PAC Profile=http://uri.etsi.org/TS102206/v1.1.3#PAC />
        </MSSP>
     <MSCD Profile= http://uri.etsi.org/TS102206/v1.1.3#MSCD >
            <Accreditation>
            CC EAL4+ PP - Secure Signature-Creation Device Type 3 Version 1.05
            </Accreditation>
        </MSCD>
    </MSS_technicalProtection>

...

</MSS_Profile>
```

7.3.3 Example 2

Here is the description of a Mobile Signature service that claims to be compliant with the European Directive Qualified Electronic Signature:

```
<MSS_Profile>
    <MSS_technicalProtection Profile=http://uri.etsi.org/TS102206/v1.1.3#MSCS >
        <MSCA>
            <conformityDeclaration>
            Manufacturer's Declaration of conformity for a Signature Creation Application
We "manufacturer's name" of "manufacturer's address" do hereby declare under our sole
responsibility...
            </conformityDeclaration>
        </MSCA>
    <MSSP>
            <DTBS Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSV />
            <DTBSF Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSF />
            <DHC Profile=http://uri.etsi.org/TS102206/v1.1.3#DHC />
            <PPC Profile=http://uri.etsi.org/TS102206/v1.1.3#PPC />
        <PAC Profile=http://uri.etsi.org/TS102206/v1.1.3#PAC />
        </MSSP>
     <MSCD>
            <Accreditation>
            CC EAL4+ PP - Secure Signature-Creation Device Type 3 Version 1.05
            </Accreditation>
        </MSCD>
    </MSS_technicalProtection>

...

</MSS_Profile>
```

Annex A: Bibliography

- EESSI: http://www.ictsb.org/eessi/EESSI-homepage.htm.
- eEurope: Global Interoperability Framework for Identification, Authentication and Electronic Signature (IAS) with Smartcards http://eeurope-smartcards.org/.
- ICTSB: http://www.ict.etsi.fr/home.htm.
- PKCS: http://www.rsasecurity.com/rsalabs/pkcs.
- UMTS: http://www.umts-forum.org/.
- WAP: http://www.wapforum.org/.
- WLAN: http://standards.ieee.org/getieee802/802.11.html.
- IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".
- IETF RFC 3369: "Cryptographic Message Syntax (CMS)".
- W3C (2001): "Web Services Description Language (WSDL) 1.1", Note 15 (http://www.w3.org/TR/wsdl).
- W3C Recommendation (2001): "XML Schema Part 1: Structures" (http://www.w3.org/TR/xmlschema-1/).
- W3C Recommendation (2001): "XML Schema Part 2: Datatypes" (http://www.w3.org/TR/xmlschema-2/).

History

Document history		
V1.1.3	August 2003	Publication