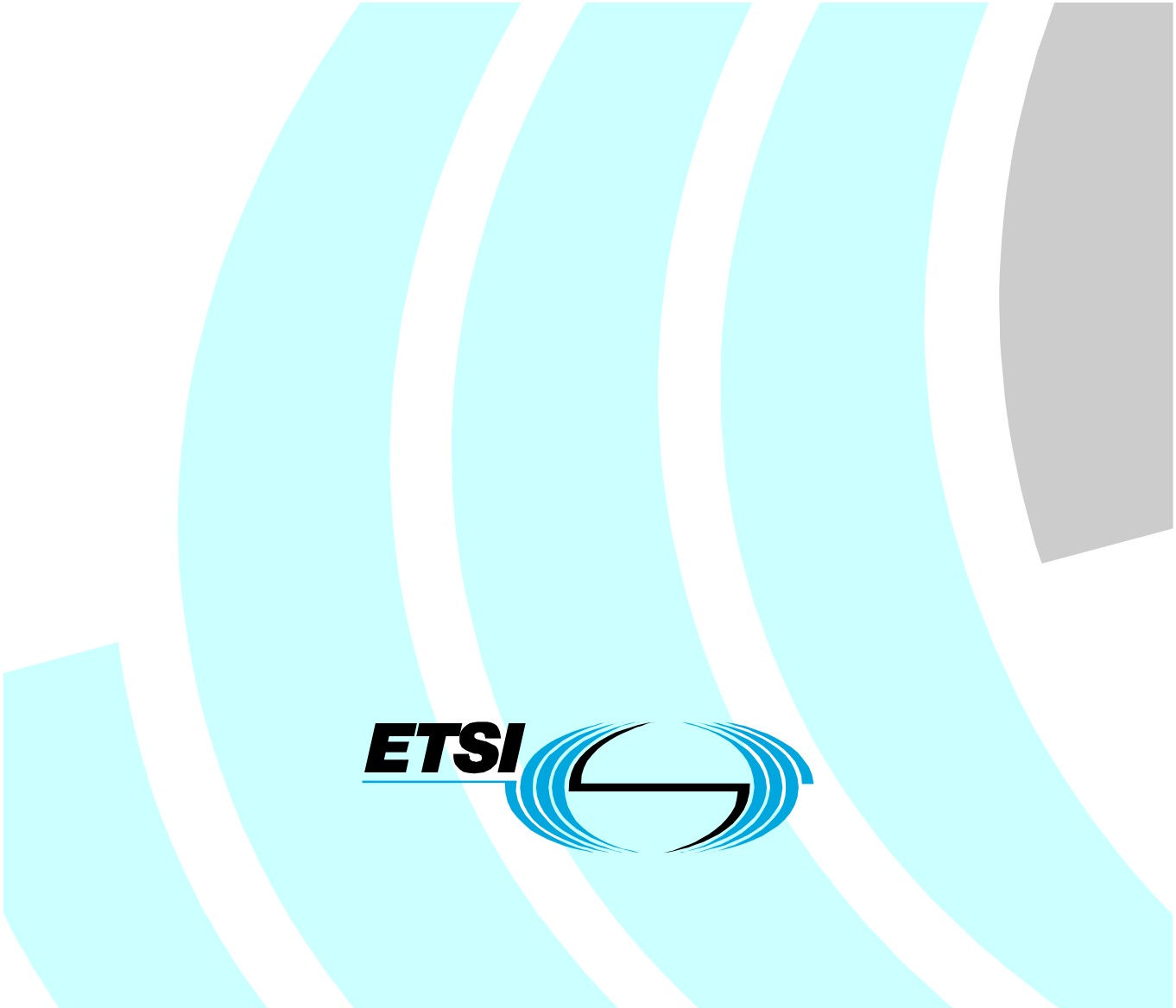
ETSI TR 102 203 V1.1.1 (2003-05)

Technical Report

Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements



Reference
DTR/M-COMM-003

Keywords
commerce, e-commerce, electronic signature,
functional, mobile

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.Notice received from:

- Swisscom

Foreword

The present document (TR) has been produced by ETSI Project M-Commerce (M-COMM).

Introduction

Structure of the present document

Scope

A description of the goals and objectives of the present document.

Document Administration

An explanation of the structure, definitions, symbols and abbreviations used in the present document.

Introduction

Positions the Mobile Signature project and EC funding etc leading to overview of why mobile signature has a way to accelerate deployment of electronic signatures as originally envisaged by the EU Directive.

Mobile Signature

Electronic signatures go mobile… definition of mobile signature.

Mobile Signature Design Criteria

Positions the criteria and technology choice for implementing mobile signature solutions.

Use Cases

Provides an overview of typical applications and services that might benefit from adoption of mobile signature to confirm the intentions of a citizen in relation to the transactional element of those applications and services. Also, describes the process sequence for some of these…

Mobile Signature Process

Outlines the end-to-end sequence involved in the mobile signature concept. The clause identifies the ACTIONS required for mobile signature to operate correctly and the ORDER in which they occur logically. An understanding of the action order helps to define what technology elements are required for the mobile signature architecture.

Mobile Signature Service

A short description of a service in which the mobile signature process is coordinated/managed.

Mobile Signature Implementation Challenges

Describes the challenges associated with implementing mobile signature service (registration and usage) in the current mobile environment. This clause identifies the starting point for:

- Task 2 = Interfaces Specification
- Task 3 = Security Provisions Specification
- Task 4 = Interoperability Specification

Roles and Responsibilities

A description of the roles identified in the mobile signature process and responsibilities of the entities that might be involved. Determination of which entity is best placed to undertake a particular role will be dependent upon the commercial model adopted.

Business and Functional Requirements

The Business requirements guide the preparation of functional requirements.

Conclusion

The present document provides guidance for drafting of ETSI Technical Specifications concerning Interfaces, Security Provisions and Interoperability required for implementation of industry-wide mobile signature services.

1 Scope

The present document ("TR") considers the business and functional requirements for a MOBILE SIGNATURE SERVICE. The present document is intended to guide the drafting of the following ETSI Technical Specifications (TS) concerning interfaces, security provisions and interoperability of mobile signatures service solutions.

- Technical Specification: TS 102 204
  - Mobile Signature Web Service Interfaces
- Technical Specification: TS 102 206
  - Security Requirements for Mobile Signature Systems
- Technical Specification: TS 102 207
  - Roaming of Mobile Signature Service Transactions

Together, the present document and the TSs will allow the design and implementation of interoperable mobile signature service solutions. As such, the present document defines business and functional requirements for mobile signature service solutions that leverage smartcards (including the GSM SIM-CARD) and cryptographic techniques (including asymmetric cryptography used in public key infrastructure - PKI) to facilitate the deployment of electronic signature solutions.

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, revocation).
- Supporting service administration and maintenance activities.

In defining the Webservice, the present document makes reference to interactions between different parties and to the end user experience of a mobile signature service at the mobile device. This is done to illustrate concepts and facilitate definition of business and functional requirements for the Webservice - only. Readers are referred to other sources of information as indicated in the "References" clause regarding definitions and specifications for these topics.

2 References

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

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

3 Definitions and abbreviations

3.1 Definitions

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

application provider: person or organization who develops and/or sells and/or supports a service used by a citizen

asymmetric cryptography: 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.

atomicity: property of a transaction, after an accidental or a malevolent interruption or shut-down the system either returns to state in which it was before the interruption or is able to carry on the interrupted task so as to complete it

buffer over-run: attack consisting in corrupting a program by overflowing its internal variables

NOTE: Can be avoided if the program checks that only data of appropriate length is stored in variables.

business case: describes the financial justification (business plan) for each commercial model

carrier groups: holding companies comprising multiple mobile network operator companies

Certification Authority (CA): authority that produces signatures on public-keys (certificates)

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

commercial model: describes roles and responsibilities of the organizations involved in providing a mobile signature service

dependent application (or service): See definition in clause 10.3.4.

dispute resolution: process of resolving disputed transactions

dual chip: mobile device containing the home network's SIM card plus a second smartcard possibly from another smartcard issuer

dual slot: mobile device capable of inserting a credit-card size smartcard

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

NOTE: Electronic signatures come are of three sorts: General, Qualified and Advanced as defined in clause 6.1.

enduser or citizen: person (or device) in possession of (or embedded in) the mobile device (and/or SIM-card) to which a mobile signature is associated

NOTE: End user and Citizen is used interchangeably throughout the present document.

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

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

mobile signature process: logical sequence of acquiring and making use of a mobile signature

mobile signature service: facility that coordinates and manages the mobile signature process represents an opportunity for the card-issuer to provide a mobile signature service to citizens and application providers

Mobile Signature Service Provider (MSSP): person or entity that provides a mobile signature service

Mobile Signature Service Provider (Home MSSP): MSSP associated to the mobile network in the citizen's normal country of residence

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

NTT DoCoMo: (specific) Japanese Telecommunication Operator

Prepaid Top-UP: act of adding service credits to a pre-paid account

proof of possession: proof that the citizen possesses or owns a given mobile device

registration authority: authority in charge of capturing personal attributes from a citizen used to form the security profile

server signature: setting with which a server issues a mobile signature on the user's behalf

signature gateway: platform operated by the MSSP to enable mobile signature functionality

signing-PIN: numeric code known only to the citizen entered by that citizen on his/her mobile device keypad in order to confirm his/her intention with respect to transaction details displayed on the screen of the citizen's mobile device

NOTE: OR: A sequence of digits used to verify the identity of the holder of a token. It is a numeric "password".

signature request: message received at the citizen's mobile device from an Application Provider

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

smartcard issuer: entity who manages all aspects relating to the smartcard used to create mobile signatures (e.g. the mobile network operator)

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

tamper resistance: property of secure device, consists in resisting physical penetration attempt and avoiding leakage of secret material through various side-channels (such as time, power consumption or electromagnetic radiations)

transaction roaming: transaction where a citizen maybe using a dependent application from an AP aligned with a visited network

NOTE: In this case the visited network needs to communicate with the home network in order to obtain a mobile signature from the citizen.

trojan horse: program which apparent function is harmless (game, screen-saver, etc.) while its actual behaviour is aggressive

use case: describes the services that are enabled by mobile signature functionality

value added service: additional facility offered by an MSSP in addition to the core mobile signature

webservice: Internet technology

What You See Is What You Sign: guarantee that the message submitted to the user for approval is indeed the one that will be signed by the signing device

3.2 Abbreviations

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

AP	Application Provider
B2B	Business to Business
B2C	Business to Consumer
CA	Certification Authority
CEN	European Committee for Standardization
CSD	Circuit Switched Data
EESSI	European Electronic Signature Standardization Initiative

GPRS	General Packet Radio Service
HTTPS	HyperText Transfer Protocol Secured
ICCID	Integrated Circuit Card Identity

NOTE: The unique identifier of a particular Subscriber Identity Module (SIM) card

IVR	Interactive Voice Response (system)
J2ME	Java 2 Micro Edition
LAN	Local Area Network
MAC	Message Authentication Code
MNO	Mobile Network Operator
m-Signature	Mobile Signature
MS-ISDN	The calling number for a citizen's mobile device.
MSSP	Mobile Signature Service Provider
OMA	Open Mobile Alliance
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	PIN Unblock Key

NOTE: If a wrong PIN is given a certain number of times, it is blocked. A PUK is needed to unblock the use of the PIN.

RA	Registration Authority
SigREQ-STD	Signature request received by an MSSP from an AP.
SigRESP-STD	Response to a SigREQ-STD
SIM-Card	The smartcard located inside a mobile telephone used to manage the subscriber's access to the mobile telephone network. The spare available memory on the SIM-card is often used to provide other services to the subscriber (e.g. telephone address book).
SMS	Short Message Service
SSL	Secure Socket Layer
STF-221	ETSI Specialist Task Force 221
STK	SIM Toolkit
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telephone System
USSD	Unstructured Supplementary Services Data
WAP	Wireless Application Protocol

4 Void

5 Background

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. Consequently, communications networks of all kinds are being exploited in new ways to conduct business, to facilitate remote (tele-) 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 [1]) 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 secure systems, including "secure signature creation devices". To date (May 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" (Note: What-You-See-Is-What-You-Sign). 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 a convenient choice for implementation of a socially-inclusive, electronic signature solution for the majority of citizens.

Electronic signatures created in this way are defined in the present document 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.

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 the present document and Technical Specifications for a:

- 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 a facility (to be known as mobile signature service) which will allow application providers of any kind to present mobile signature requests to the citizen's mobile and to receive a mobile signature in response.

6 Mobile Signature

6.1 Electronic Signatures Go Mobile

"I am… my cellphone."

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:

- General

  Any electronic signature that is not a "qualified" electronic signature. Such a signature cannot be denied legal effect, but is neither recognized automatically.

- Qualified

  An electronic signature that can be considered as the legal equivalent of a handwritten signature as a consequence of the technology used to create it.

- 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. formal confirmation that the signature was generated at a given moment).

In the context of the EU Directive, the present document (TR) considers electronic signatures created by cryptographic means in a process involving a mobile device (i.e. mobile telephone). The result - a "Mobile Signature" - can be realized by leveraging the capabilities of mobile devices (including the SIM-infrastructure) and mobile network infrastructures in a variety of ways. Whatever the implementation, the underlying principle is to obtain confirmation from a citizen that s/he wishes to proceed with a transaction, details of which were displayed for the citizen on his/her mobile phone screen.

6.2 Proposed Definition for "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 (see 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.

6.3 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.

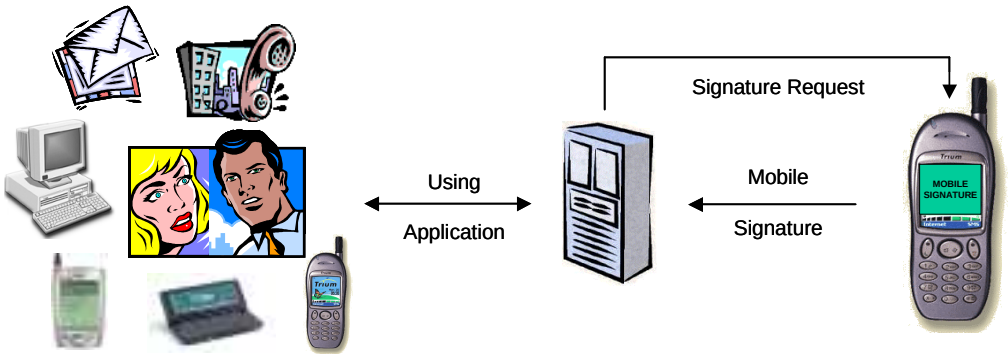


Figure 1: Mobile Device as "Signing Tool" (An Electronic Pen…)

In considering the use of mobile signature, the present document considers 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.

7 Mobile Signature Design Criteria

The concept of a mobile signature is attractive because it leverages existing commercial models, network infrastructure, mobile device technology and customer relationships managed by GSM mobile network operators.

Mobile telephones and network infrastructures provide scope and opportunity to realize mobile signature functionality in two main "generic" ways; Server-Side and Smart Card-based implementations. Either implementation possibility may make use of any of the mobile network communications bearer mechanisms (e.g. USSD, SMS, Circuit Switched, GPRS, UMTS, etc.) and various protocols (e.g. WAP) in conjunction with a suitable "signing" application in the mobile device that can be addressed by an application or service being used by a citizen.

7.1 Server-Side Designs

In **server-side implementations**, signature creation is achieved with a secure server engineered in the mobile network infrastructure (i.e. a signature "proxy" or "gateway"). The creation of a mobile signature in these implementations is initiated by receipt of an appropriate code (e.g. a message authentication code - MAC) from the mobile device following PIN-code entry using the mobile device keypad. The code triggers signature creation by the server.

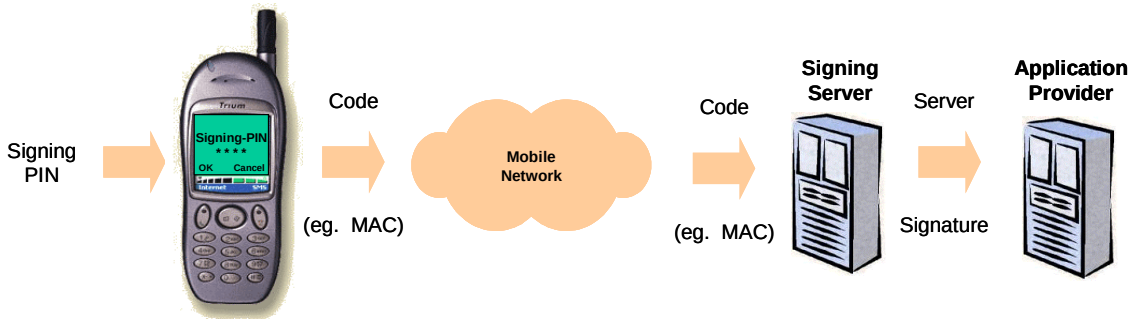


Figure 2: Typical Server Side Implementation

These kind of implementations are interesting because of their "simplicity" and many of the elements are common with smart-card based designs, described below. However, issues surrounding the suitability of a server as a signature creation device (as defined in the European Directive) may prevent the creation of advanced electronic signatures. In addition, in some scenarios (e.g. typically with MAC codes) it may be possible to generate a mobile signature at the signing server without entry of the Signing-PIN by the citizen. Such an approach may be appropriate in some cases, but results in the creation of a server signature rather than a mobile signature.

A fundamental difference of server-side "signature by proxy" from local (smart card-based) signatures is that proxy-generated signatures cannot provide the highest degree of confidence that a signature is valid. Such signatures may be perfectly acceptable in many applications, however some applications (such as high-value financial transactions or those controlling access to highly sensitive information) may require signatures which are generated using secret material held solely by the signing party in a physically and logically secure device.

7.2 Smart-Card Based Designs

In **smartcard based implementations**, signature creation is achieved using a crypto-processor on a smartcard, such as the subscriber identity module (i.e. SIM-card) found inside GSM mobile handsets or the Universal Integrated Circuit Card (UICC) that has been adopted for 3rd Generation mobile devices. The use of SIM or UICC smartcards in the mobile operator business model effectively places mobile operators in the role of "Smartcard Issuer".

Figure 3: Typical Mobile Smartcard Implementation

Signature requests received at a citizens' mobile device trigger a "signing" application on a smartcard. This allows display of the transaction text on the mobile device screen and provides the option for the citizen to enter his/her signing-PIN. The act of entering the correct signing-PIN initiates creation of the mobile signature in the smartcard and transmission of the signature to the mobile signature service. By entering the correct signing-PIN, the citizen is deemed to have confirmed his/her intention to proceed with the transaction details displayed on his/her mobile device screen.

The extensive ownership of GSM mobile handsets (Note: 800 million GSM users in an estimated total subscriber base of 1,2 billion users) provides an ideal smart-card platform on which to design mobile signature capability. Particularly as the evolution of GSM mobile telephony into the so-called 3rd Generation (UMTS) has itself adopted similar integral smartcard technology in the form of UICC. This approach makes other technologies such as specialist dual-slot or dual-chip terminals largely confined to particular "communities-of-interest".

7.3 Choice of Cryptographic Techniques

Both symmetric and asymmetric cryptography techniques may be suitable to support the creation of mobile signatures.

Symmetric key techniques have the advantages of using algorithms which are simple to implement on low-cost, computational devices. Key generation is also straightforward and the implementation of symmetric key schemes does not require highly specialized knowledge. However, by definition, the use of the same key by two entities provides scope for any transaction to be disputed, with associated costs for resolution. In addition, key management issues arise as the number of participating entities increases.

Asymmetric key techniques require higher cost computational devices and produce responses of greater size, but allow the same "key-pair" to be adopted in multiple relationships. The use of a "key-pair" in which one of the keys is always associated with one citizen provides the opportunity for greater scalability and easier dispute resolution. Such an approach results in a more effective trust model with opportunities for simplified administration and operational management (e.g. Many applications and many relationships can be supported by a single asymmetric key pair). As a consequence, documents describing global interoperability frameworks for electronic signature (e.g. eEurope "Blueprint" Smartcard Initiative) almost exclusively focus on the asymmetric cryptographic technique.

The present document makes no pre-assumptions concerning the cryptographic choice and neither technique is specifically excluded. However, the listing of business and functional requirements (clause 14) makes provision for both symmetric and asymmetric technique.

7.4 Public Key Infrastructure (PKI) Technology

PKI technology makes use of asymmetric cryptography to create a link between two distinct (different) keys owned by a citizen; a "public" key whose identity is readily available and a "private" key stored securely in a tamper resistant device (such as a smartcard). The mathematical relation between the keys is such that an action completed with one key can be linked to the other key but without revealing the private key data. This is particularly useful for creating an electronic signature, since the signing action completed by a private key identifies the private key owner only by virtue of the relationship with the associated public key - the identity of which is known.

The important elements of using PKI technology are to ensure that a private key remains "private" and to validate that a public is actually associated with a particular private key. This is achieved by closely managing the registration process by which keys are issued and by operating a certification scheme that confirms the validity of the public key identity. These elements are managed respectively by entities known as "Registration" and "Certification" Authorities, (i.e. RA and CA). In relation to mobile signature, their primary function is to acknowledge the unique relationship between private key usage and the registered identity of a citizen by virtue of his/her ownership of the associated public key.

7.5 Technology Choice

The present document focuses on those technologies able to realize a mobile signature equivalent of an "electronic signature" as defined by the European Directive. In designing a mobile signature architecture, public key infrastructure technology can be combined with the SIM-card (or UICC), a suitable mobile device and any of the mobile network elements. This will allow various implementations to be considered based on a modular, or layered, approach (e.g. SMS/STK/PKI; GPR/WAP/WIM/PKI, etc.).

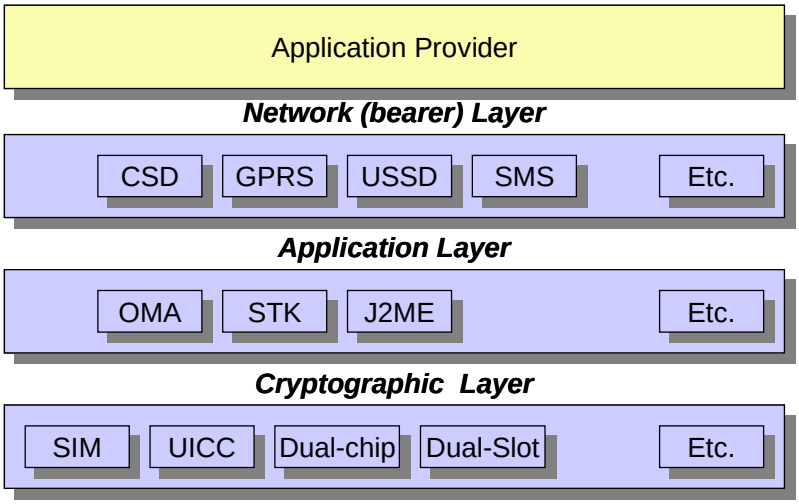


Figure 4: Modular Approach of Mobile Signature

Technology choice is a matter for the mobile operator - or a third party which has a relationship with an operator - provided that the degree of confidence required by the parties who will rely on the mobile signature for whatever reason is satisfied. Some parties may require a higher degree of confidence for higher value transactions and vice versa. In this context, "value" is measured in terms of consequence (including damage to brand equity) as well as monetary amount. Security provisions are detailed in Task 3 of this special task force.

8 Use Cases for Mobile Signature

8.1 Potential Use Cases

A use case is a description of a situation or service in which the mobile signature "signing" functionality is used to participate in the completion of a transaction. Generically, use cases could either:

- Supplement "traditional" smartcard/cardreader implementation (citizen present).
- Particularly "remote" and "electronic" applications (citizen not physically present).

Mobile signature provides a facility that could be used to enable all kinds of potential use cases. However, care needs to be exercised when examining service proposition ideas for practicability - how does a mobile signature resolve a significant problem or enhance the current situation? Only appropriate use cases will drive adoption of mobile signature capability and support implementation of the European Directive on Electronic Signature.

Since a mobile signature is defined as…

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

… mobile signatures can be used either to supplement existing security arrangements, or as the primary security mechanism for identity management in the following scenarios:

- Citizen Present

  A face-to-face situation (e.g. point-of-sale) with either another person or a piece of machinery (e.g. a vending machine, parking meter, etc.) to confirm a transaction instruction.

- Citizen Not Present

  Situations where the citizen is using either "remote" (e.g. a telephone call) or "electronic" (e.g. computer-based) means to confirm a transaction instruction.

Since transaction instructions can be confirmed by a citizen (or by a machine) to other people or machines, the following classification system provides a convenient way to categorize a selection of potential use cases:

- Person-to-Person
- Person-to-Machine
- Machine-to-Person
- Machine-to-Machine

A selection of potential use cases are indicated in table 1. These are provided for illustrative purposes only and no opinion is offered as to the appropriateness of each use case suggested.

Table 1: Use Case Classification System

	Person	**Machine**
Person	Messaging Email Instructions Location Confirmation Auction Purchase Approval Requests Business Expenses Debit Card Telephone Order Proof of Age Contract Confirmation Personal Credential Proof Of Membership Delivery Instructions Payment Instructions	Prepaid Top-Up Vending machine purchase Car park payment Disable an alarm system Access to controlled information Health/medical records Ticketing Airline Check-In Betting/gaming/gambling LAN Access control Website/webpage access Voting Physical Access (e.g. Garage Door) Electronic/online shopping Delivery instructions Payment instructions
Machine	Secure Download Content / Software Distribution Digital Rights Management Share Trading Bill Payment Funds Transfer	Road Tolls Other telemetry (meter reading) Vending machine orders replacement stock items Wireless-LAN (802.11x) Software Distribution

A number of specific examples are taken to illustrate the mobile signature concept in use:

- Person-to-Person.

  Personal credential (e.g. in lieu of passport).

- Person-to-Machine.

  Debit Card Top-Up of Prepaid Accounts.

- Machine-to-Person.

  Content Download (e.g. protection of minors), etc.

- Machine-to-Machine.

  Automated stock replenishment instructions (e.g. vending machines), etc.

8.2 Sample Mobile Signature Enabled Use Cases

Some of the potential use cases from the table above are described in this clause as a process flow. This allows the mobile signature "routine" to be identified and positioned as a standard element in each scenario. A generic template can be found in annex A.

8.3 Customer Initiated Top-Up of Prepaid Accounts

In this use case, mobile signature is proposed as a way of obtaining a citizen's permission to use a registered payment means to **initiate** the process of acquiring additional service credits. Once initiated, existing payment methodologies can be invoked, perhaps to replace voucher schemes altogether (which are prone to fraud and which attract high overheads on the face value of service credits). Adding a mobile signature element to the process places control of payment means usage in the hands of the rightful owner.

CUSTOMER INITIATED TOP-UP of PREPAID ACCOUNTS by DEBIT CARD	
Service Proposition:	Citizen uses his/her mobile signature to confirm intention to use a registered payment means to purchase additional pre-paid service credits.
Service Type:	Person-to-Machine (citizen initiated)
Market Segment:	B2C
Target Market:	ALL CITIZENS with PRE-PAID ACCOUNTS
PRE-CONDITIONS	
Condition:	Description
A	Citizen has acquired mobile signature capability.
B	Citizen has registered to use this application.
C	Citizen has registered a debit card payment means with the service operator.
D	Citizen decides to increase his/her service credit.
Description Of Service	
Step:	Description
1	Citizen initiates the "top-up" process by any of the accepted, current, application channel (e.g. CSD/GPRS WAP session, PC/TV-internet, voice call to IVR platform, etc.).
2	Citizen provides ID for top-up account (Note: for mobile phone prepaid services this is the MS-ISDN).
3	Citizen confirms the amount of service credit s/he wishes to acquire.
4	Citizen confirms which payment means to complete to the "top-up" transaction (e.g. the registered debit card).
5	Pre-paid system (e.g. an "Intelligent Network" platform) prepares a payment instruction plus an associated mobile signature request (a short form version of the transaction containing key details of the transaction - the text to be "signed").
6	Prepaid system forwards mobile signature request to mobile signature service.
7	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).
8	Valid mobile signature request… …the mobile signature request transferred to citizen's mobile device.
9	Mobile signature request received at citizen's mobile device.
10	Citizen reads content of the received mobile signature request.
11	Citizen follows on-screen instructions and enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.
12	Mobile device returns mobile signature to prepaid system.
13	Mobile signature service returns a POSITIVE *(i.e. "mobile signature successful")* condition response to the Pre-paid system.

CUSTOMER INITIATED TOP-UP of PREPAID ACCOUNTS by DEBIT CARD	
14	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.
15	Pre-paid system uses mobile signature response to inform the "top-up" decision and initiate associated actions (e.g. the payment instruction).
16	Payment instruction processed successfully and prepaid system authorized to credit the citizen's account with the requested amount.
17	Transaction completion receipt (e.g. "Top-Up" completed) notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
18	USE CASE ENDS.

8.4 Corporate Local Area Network (LAN) Access

Because:

- Allows LAN Access Control from any web-browser.
- Removes need for dedicated security solution to control LAN Access.
- Removes need for dedicated dial-up access solution.

WEB ACCESS CONTROL to COPORATE LAN	
Service Proposition:	Mobile signature confirms identity (and hence access rights) of citizen attempting to gain access to a corporate local area network.
Service Type:	Person-to-Machine
Market Segment:	B2B
Target Market:	CORPORATE MARKET
PRE-CONDITIONS	
Condition:	Description
A	Citizen is an authorized user of the corporate local area network.
B	Citizen has acquired mobile signature capability.
C	Citizen has registered to use this application.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	
Step:	Description
1	Citizen establishes a MODEM connection to the corporate LAN.
2	LAN Access control application requests user information.
3	Citizen enters Username and Password, plus MS-ISDN.
4	LAN Access control application prepares logon script and an associated mobile signature request containing the text to be signed (Note: to be used to authorize the logon script). Example: "Username has requested logon to LAN. Do you approve this logon request?" [Please enter Signing-PIN etc].
5	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).

WEB ACCESS CONTROL to COPORATE LAN	
6	Valid mobile signature request… …the mobile signature request transferred to citizen's mobile device.
7	Mobile signature request received at citizen's mobile device.
8	Citizen reads content of the received mobile signature request and follows on-screen instructions to generate his/her mobile signature.
9	Citizen enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.
10	Mobile device returns mobile signature to mobile signature service.
11	Mobile signature service processes mobile signature received from citizen's mobile device.
12	Mobile signature service returns a POSITIVE *(i.e. mobile signature successful")* condition response to the LAN Access Control application.
13	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.
14	LAN Access Control application uses mobile signature response to inform the logon decision and initiate associated actions (e.g. the logon script).
16	Transaction completion receipt (e.g. LAN logon completed) notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
17	USE CASE ENDS.

8.5 Content Download

Because:

- Mobile signature provides positive enduser identification to inform "download" decision.
- Content provider can demonstrate active attempt to prevent inappropriate content download to minors.

CONTENT DOWNLOAD	
Service Proposition:	Content server requests citizen to provide his/her mobile signature to initiate download (content transfer) process.
Service Type:	Person-to-Machine
Market Segment:	B2C
Target Market:	ALL (e.g. YOUTH SEGMENT)
PRE-CONDITIONS	
Condition:	Description
A	Citizen has acquired mobile signature capability.
B	Citizen has registered with the content provider.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	

CONTENT DOWNLOAD	
Step:	Description
1	Citizen accesses the content provider's portal by any of the current application channels (e.g. PC/TV-internet, voice call to IVR platform, mobile CSD/GPRS WAP session,, etc.).
2	Citizen selects preferred content and requests download.
3	Content server prepares a download script and an associated mobile signature request containing key details of the text to be signed (e.g. content name and type, confirmation by citizen that s/he is of "qualifying age"…). Example: "You have requested download of ***"content-name"***. Do you approve this download request?" [Please enter Signing-PIN etc].
4	Content server forwards mobile signature request to mobile signature service.
5	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).
6	Valid mobile signature request… …the mobile signature request transferred to citizen's mobile device.
7	Mobile signature request received at citizen's mobile device.
8	Citizen reads content of the received mobile signature request and follows on-screen instructions to generate his/her mobile signature.
9	Citizen enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.
10	Mobile device returns mobile signature to mobile signature service.
11	Mobile signature service processes mobile signature received from citizen's mobile device.
12	Mobile signature service returns a POSITIVE *(i.e. mobile signature successful")* condition response to content server.
13	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.
14	Content server uses mobile signature response to inform the "download" decision and initiate associated actions (e.g. the download script and, perhaps, a payment instruction).
15	Content is downloaded to citizen via application channel.
16	Transaction completion receipt (e.g. content download completed) notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
17	USE CASE ENDS.

8.6 Automated Prepaid Service "Top-Up"

Because:

- Overcomes potential "mis-use" of registered payment means.

AUTOMATED PREPAID SERVICE "TOP-UP"	
Service Proposition:	Threshold value in prepaid system triggers an automated "top-up" sequence to request citizen permission to purchase service credits using a registered payment means (e.g. a debit card).
Service Type:	Machine-to-Person
Market Segment:	B2B
Target Market:	ALL CITIZENS with PRE-PAID ACCOUNTS
PRE-CONDITIONS	
Condition:	Description
A	Citizen has acquired mobile signature capability.
B	Citizen has registered to use this application.
C	Citizen has registered a payment means (e.g. a debit card) with the service operator.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	
Step:	Description
1	Prepaid account decrements to the pre-configured "threshold" value.
2	Prepaid system applies minimum service credit purchase rules or retrieves prepaid account holder's preferences from file (e.g. maximum service credit purchase).
3	Prepaid system prepares a payment transaction instruction and an associated mobile signature service request containing the text to be signed (Note: to be used as the citizen's permission to action to the payment instruction).
4	Mobile signature request received by mobile signature service.
5	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).
6	Valid mobile signature request… …the mobile signature request transferred to citizen's mobile device.
7	Mobile signature request received at citizen's mobile device.
8	Citizen reads content of the received mobile signature request and follows on-screen instructions to generate his/her mobile signature.
9	Citizen enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.
10	Mobile device returns mobile signature to mobile signature service.
11	Mobile signature service processes mobile signature received from citizen's mobile device.
12	Mobile signature service returns a POSITIVE *(i.e. "mobile signature successful")* condition response to prepaid system.
13	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.

AUTOMATED PREPAID SERVICE "TOP-UP"	
14	Prepaid system uses mobile signature response to inform the "top-up" decision and initiate associated actions (e.g. the appropriate payment methodology).
16	Transaction completion receipt (e.g. account "top-up" completed) notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
17	USE CASE ENDS.

8.7 Machine Maintenance Request (Alarm Conditions)

This use case is provided to stimulate discussion. The reader will note that contrary to the other use cases described here, no signing-PIN is required by the machine. The use case is offered because it may:

- Allow positive identification of machine identity (and hence location).
- Defeat fraudulent "impersonation" of machine.

MACHINE MAINTENANCE REQUEST / ALARM CONDITION	
Service Proposition:	Remotely located "machines" (e.g. vending machines) issue genuine maintenance requests to service company: Out-of-stock Cash related (e.g. please empty me!) Cash related (e.g. please provide more coins of type X) Other alarm condition exists
Service Type:	Machine-to-Machine
Market Segment:	B2B
Target Market:	Telemetry and Telematics
PRE-CONDITIONS	
Condition:	Description
A	Machine equipped with GSM mobile data capability.
B	Machine equipped with mobile signature capability.
C	Machine equipped with GSM mobile data capability.
D	Machine registered for application.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	
Step:	Description
1	Remote machine automatically detects threshold value and/or alarm "condition".
2	Remote machine prepares telematic status report for detected "condition".
3	Remote machine generates mobile signature.
4	Mobile signature attached to status report.
5	Remote machine transmits signed message to central maintenance server.
6	Central maintenance server creates mobile signature verification request.
7	Mobile signature verification request forwarded to mobile signature service.

MACHINE MAINTENANCE REQUEST / ALARM CONDITION	
8	Mobile signature service verifies validity of mobile signature.
9	Mobile signature service returns response to central server.
10	Central maintenance server uses mobile signature verification to inform service maintenance decisions.
11	Transaction completion receipt (e.g. service request) notified to machine's mobile signature webpage (i.e. service log).
12	USE CASE ENDS.

8.8 Disable Alarm Protection System

Because:

- Allows remote instruction to be processed without invalidating insurance provisions

REMOTE CONTROL of ALARM PROTECTION SYSTEMS	
Service Proposition:	Citizen uses mobile signature to remotely control an alarm protection system following a request from an authenticated party (e.g. to allow a citizen who cannot be present physically to disable the system in the case where access is required by a keyholder who has authenticated him/her-self by mobile signature).
Service Type:	Person-to-Machine-to-Person-to-Machine
Market Segment:	CONSUMER + CORPORATE
Target Market:	ALARM SYSTEM KEYHOLDERS
PRE-CONDITIONS	
Condition:	Description
A	Citizen is registered keyholder for the alarm protection system.
B	Citizen and Requesting Party have both acquired mobile signature capability.
C	Requesting party (or his/her organization) is known to the citizen and, perhaps,
C	Citizen has registered to use this application.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	
Step:	Description
1	*An alarm monitoring service or other agency (e.g. the Police) contacts the citizen.*
2	*Citizen agrees to disable alarm system.*
3	*An alarm monitoring service* application prepares *a disable instruction* and an associated mobile signature request containing the text to be signed (Note: to be used to authorize the disable instruction).
4	Mobile signature request received by mobile signature service.
5	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).
6	VALID mobile signature request… …the mobile signature request transferred to citizen's mobile device.
7	Mobile signature request received at citizen's mobile device.

REMOTE CONTROL of ALARM PROTECTION SYSTEMS	
8	Citizen reads content of the received mobile signature request and follows on-screen instructions to generate his/her mobile signature.
9	Citizen enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.
10	Mobile device returns mobile signature to mobile signature service.
11	Mobile signature service processes mobile signature received from citizen's mobile device.
12	Mobile signature service returns a POSITIVE *(i.e. "mobile signature successful")* condition response to *the alarm monitoring service* application.
13	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.
14	*The alarm monitoring service* application uses mobile signature response to inform the transaction instruction decision and initiate associated actions *(e.g. the disable instruction).*
16	Transaction completion receipt *(e.g. the disable instruction)* notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
17	USE CASE ENDS.

8.9 Stock/Share Trading

Because:

- In this use-case, the application provider (e.g. a stockbroker) requires permission from the citizen to execute a "buy" or "sell" instruction.

STOCK/SHARE TRADING	
Service Proposition:	Pre-configured threshold value in stocks/shares system or a "buy/sell" recommendation triggers a mobile signature request to authorize purchase (or sale) of stocks/shares.
Service Type:	Machine-to-Person
Market Segment:	B2C, B2B
Target Market:	Stock/share-owning citizens.
PRE-CONDITIONS	
Condition:	Description
A	Citizen has acquired mobile signature capability.
B	Citizen has registered to use this application.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	
Step:	Description
1	A stock/share price reaches a threshold value configured by the citizen (or a "buy/sell" recommendation is prepared by the citizen's stockbroker).

STOCK/SHARE TRADING	
2	Stockbroker application triggers an alert message to the citizen's mobile device, prompting the citizen to contact the stockbroker call centre (or view a WAP-site, web-site, etc.).
3	Citizen confirms details of his/her transaction instruction.
4	Stockbroker application prepares a stock/share trade instruction and an associated mobile signature service request containing the text to be signed (Note: to be used as the citizen's permission to action to the stock trade instruction).
5	Mobile signature request received by mobile signature service.
6	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).
7	VALID mobile signature request… …the mobile signature request transferred to citizen's mobile device.
8	Mobile signature request received at citizen's mobile device.
9	Citizen reads content of the received mobile signature request and follows on-screen instructions to generate his/her mobile signature.
10	Citizen enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.
11	Mobile device returns mobile signature to mobile signature service.
12	Mobile signature service processes mobile signature received from citizen's mobile device.
13	Mobile signature service returns a POSITIVE *(i.e. mobile signature successful")* condition response to stockbroker application.
14	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.
15	Stockbroker application uses mobile signature response to inform the transaction instruction decision and initiate associated actions (e.g. the stock/share trade instruction).
16	Transaction completion receipt notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
17	USE CASE ENDS.

9 Mobile Signature Process

The process of acquiring and using a mobile signature involves the following logical sequence:

- Awareness: … where citizens are made aware of mobile signature and those applications/services requiring mobile signature capability.
- Mobile Signature Acquisition: … the process of equipping citizens to make use of mobile signature (includes registration for signing capability, activation of "signing" functionality in the citizen's mobile device, registration for service(s) requiring mobile signature and completion of associated administration).
- Use of Mobile Signature: … processing of mobile signature requests and generation of mobile signatures at the mobile device.
- Mobile Signature Lifecycle Management: … management of all elements comprising the mobile signature solution, including signature lifecycle (e.g. validity period, expiry, revocation, etc.).
- Customer Service: … assisting citizens and APs alike in the ongoing use of mobile signature and resolving any administrative issues that may arise.

A short description is provided for each process step, with further explanation given in clause 10.

9.1 Awareness

The "awareness" process step includes all aspects of advertising and providing information concerning mobile signatures and their use. During this step, it is imperative that citizens are presented with information in a way which sets the correct expectations and which clearly explains the citizen's responsibilities and the consequences of using mobile signatures.

9.2 Mobile Signature Acquisition

The "acquisition" phase concerns all aspects relating to equipping a citizen to use mobile signature capability. Logically, it involves a four stage process:

- Deployment of mobile signature equipment.
- Creating a citizen's security profile that supports signing capability (i.e. a user registration process).
- Activating "signing" functionality at the mobile device.
- Registering to use an application/service that requires mobile signature capability (a "dependent" application).

9.3 Use of Mobile Signature Capability

Mobile signature capability describes the ability of a citizen to provide a mobile signature in response to a request from an application provider (i.e. the core facility). It is of use to both citizens and the application providers who rely on a citizen's mobile signature for whatever reason.

9.3.1 By an Application Provider

Use of a dependent application by a citizen may initiate use of his/her mobile signature. In this case, the AP needs to prepare a transaction instruction and an associated mobile signature request containing the text to be signed by the citizen. Mobile signature requests are forwarded to the citizen's mobile device via the mobile operator using an appropriate interface. Mobile signature responses - depending on various conditions - are returned to the AP using the same interface.

9.3.2 By a Citizen (Cardholder)

Before a citizen can use his/her mobile signature capability, s/he must first have acquired the signing capability and be using a "dependent" application or service for which mobile signature "signing" functionality is recognized and accepted by an AP. On receipt of a mobile signature request from an AP, the request should be displayed automatically on the mobile device screen (i.e. without Enduser intervention). The request should include the key aspects of the transaction for which the AP has requested a mobile signature, such that the citizen may make an appropriate determination of whether to sign the request (or not). Where a citizen wishes to provide his/her permission to the AP to proceed with the transaction, the citizen will enter his/her "Signing-PIN" code via the mobile device keypad and trigger creation of his/her mobile signature. In all cases where a citizen provides his/her mobile signature, it is recommended that s/he will be provided with positive confirmation of the outcome of the "signing" act (e.g. success/fail). This confirmation will be provided by the MSSP or the AP and its meaning might be application-dependent.

Use of mobile signature may be accompanied by a range of value added services provided to citizens and APs alike by the MSSP. These are described further in clause 10.

9.4 Mobile Signature Lifecycle Management

Once a citizen has acquired mobile signature capability, its continued use requires management. This may involve:

- Replacement/update of mobile signature equipment: SIM-card.
- Replacement/update of mobile signature equipment: Mobile Devices.
- Update of registration information(s).
- PIN-code management.
- Certificate revocation.

9.5 Customer Service

Customer service is a key aspect that will help to determine the continued use of mobile signature capability by citizens and APs. Wherever the call for assistance is received, the call centre representatives should be able to assist the caller appropriately. This might involve providing an immediate resolution, or in referring callers to the correct party, depending on the nature of the service request (e.g. problems with application usage might be referred to the application provider).

10 Mobile Signature Service

Coordination and management of the mobile signature process represents an opportunity for the card-issuer (e.g. mobile network operator) to provide a MOBILE SIGNATURE SERVICE to 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 12. It is worthwhile noting at this point that legal issues are important but given the variety of national laws that govern such commercial agreements further investigations in this area would demand considerable resources that we do not have for the time being.

10.1 Mobile Signature Service - Web Service

It is envisaged that the majority of services offered by MSSPs may be provided using approaches and technology that is commonplace in the internet environment, such as "webservices". This should allow adoption of a standard interface (i.e. a universal API) for all mobile signature services, irrespective of the provider and is considered in more detail in Clause 13.

10.2 Facilitating Awareness

The "awareness" process step includes all aspects of advertising and providing information concerning mobile signatures and their use, including;

- setting the correct citizen expectations.
- explaining the use of mobile signature (in non-technical language).
- outlining minimum requirements (e.g. mobile device, subscription type, etc.).
- explaining the citizen's responsibilities and consequences of using mobile signatures.
- describing the process of acquiring mobile signature capability.
- identifying other product attributes and value-added services.
- indicating contact details for the citizen to seek additional advice and guidance.
- Provision of a messaging function to allow the citizen to seek clarification.

This information could be provided to citizens through an MSSP's website, which might also be used to facilitate call centre and retail store activities (where the webpages might form part of the MSSPs intranet).

10.3 Facilitating Mobile Signature Acquisition

In all cases, the webservice shall be capable of facilitating the mobile signature acquisition process. It may be operated by the citizen directly (e.g. website access) or by an authorized representative of the MSSP operating the website on the citizen's behalf (e.g. Telephone helpdesk, retail store visit). Depending on who is operating the webservice, the acquisition process may vary in some respects - described later.

- Telephone helpdesk.
- Website access (TV, PC, mobile devices).
- Retail store visit.

The method used by a citizen to acquire mobile signature capability should be identified in some way (in order to inform APs (relying parties). This may be important for APs who prefer the acquisition process to have been completed by the citizen in person, where positive verification of the citizen's identity was achieved in accordance with any contract [TERMS and CONDITIONS] between AP and MSSP.

10.3.1 Mobile Signature Equipment Deployment

Mobile signature equipment comprises a suitable mobile handset containing a smartcard (e.g. SIM-card) and is supplied ("issued") by mobile network operators and their distribution channel partners. Unknown to the citizen, the SIM-card may already contain a "signing" application, a cryptographic processor and a "signing" key. It is understood that the present document does not exclude the possibility of implementing electronic signatures by leveraging dual slot technology.

10.3.2 User Registration

During this step, a citizen will be required to provide sufficient personal information that verifies who the citizen claims to be. This activity is managed by a Registration Authority (RA) acting on behalf of the Certification Authority (CA) who will confirm (i.e. certify) the existence, validity and ownership of the cryptographic parameters that will be used to create a mobile signature. In the case of asymmetric cryptography that means validity of the public keys and potential certificate support. The level of detail required of the citizen and the type of evidence needed to verify the information is normally specified by the CA. This will inform decisions concerning the degree of confidence in the mobile signature by parties who come to rely on it for whatever reason.

The consequence of the registration process step is therefore to ensure that the citizen possesses the appropriate mobile signature equipment, plus the information that allows him/her to complete a signing act (i.e. a "Signing-PIN" code).

10.3.3 Activation of "Signing" Functionality

As the owner of the smartcard (egg SIM card), the card-issuer (e.g. the mobile network operator) has access to the signing application that resides on the smartcard and can validate the identity of the cardholder (e.g. "proof-of-possession"). This positions the card-issuer as the most appropriate entity to perform this activity.

Activation may involve:

- Personalization of a new smartcard and production of a "Signing-PIN" mailer, for delivery (Note: separately) to the citizen's registered address. The new smartcard may be despatched with signing functionality activated or in a pre-active/dormant state with appropriate instructions.
- Activation of a (pre-active/dormant) mobile signature application on the smartcard.
- Key generation processes and, where appropriate, generation, storage and publication of supporting certificates.

In all cases, the citizen may be required to be an active participant in the activation process. This might involve configuring some information at the mobile device (e.g. selecting his/her own "Signing-PIN") in a menu-led sequence, or providing a mobile signature in response to a MSSPs "test" application. The response to the test application may itself trigger completion of the activation process (e.g. publishing of public key data in PKI implementations).

10.3.4 Registration for a "Dependent" Application

"A "dependent" application (or service) is one that requires a citizen to possess mobile signature capability in order to complete the transactional element of that application. Without "signing" capability, the application may not function correctly."

A citizen may choose to register to use a dependent application directly with an Application Provider (AP) or via his/her mobile network operator. Registration may be completed in the following ways:

- By telephone (i.e. a voice call)
- By Internet
- In person at an AP's premises

During the registration process, the AP may determine that the citizen has active mobile signature capability with an appropriate security profile conferring the required degree of confidence in his/her mobile signature. In cases where a citizen's security profile is not acceptable, the AP itself may facilitate creation of an alternative security profile. Alternatively, the AP may terminate the registration process.

10.4 Use of Mobile Signature Capability

Mobile signature capability consists of the core signing service (i.e. the ability to provide a mobile signature) and, perhaps, a range of value added services (such as a personal webpage or other services described later) offered by a particular MSSP.

10.4.1 By the Application Provider (AP)

The webservice shall process signature requests [SigREQ-STD] received from APs and return the appropriate signature response [SigRESP-STD] to the correct requesting party. This may involve a translation from the "standard" request format into an operator-specific format and vice versa for the response.

Commercial agreements between APs and MSSPs may define the degree of confidence and quality of service conditions governing the use of the mobile signature service provided by the MSSP. In situations where no such agreement exists (e.g. a previous commercial agreement expires), MSSPs may choose not to process signature requests received from APs or to process requests entirely at the APs risk.

APs will be provided with sufficient technical information concerning the Applications Programming Interface (API) required to allow their application to make successful signature requests and to receive signature responses to/from their MSSP. Processing of the responses by APs is outside the scope of the present document.

Communications channels between APs and MSSPs may use a secure web connection as defined in Task 3 (security provisions) to satisfy commercial agreements etc.

All signature requests and responses will trigger an appropriate acknowledgement to indicate that each process instruction has been received and understood and is capable of being processed. Status updates will be provided periodically (e.g. Awaiting response from "foreign" MSSP).

All signature requests shall have a "time-out" period and "time-out" acknowledgements provided to requesting parties. A "time-out" may invoke a "re-try" policy, subject to the validity period for the transaction.

Where a signature response cannot be provided by a MSSP, a signature request "fail" message shall be provided to the requesting party, along with an appropriate error message describing the reason for failure.

Signature responses provided by the MSSP to a requesting party shall include information allowing to unambiguously determine the properties and parameters of the mobile signature received from the enduser. The AP shall be provided with sufficient information to inform his/her decision to proceed with the enduser transaction.

The following conditions are required:

SigREQ (AP to MSSP)

- Format (to be defined in Task 2).
- Use of existing standards where they exist is encouraged.
- MS-ISDN in international format recommended. However, an independent identifier, which may be mapped to a MS-ISDN by the MSSP, may be used instead of the MS-ISDN itself.
- The signature request should be presented to the citizen in the language of the citizen's preference.
- Citizen's must be able to make a meaningful determination of the transaction details in keeping with the principle "What-you-see-is-what-you-sign (and understand)" also noted in clause 12.3.

MSSP Acknowledgement towards AP

- Processing - please wait.
- Timeout - not able to get an acknowledgement from MSSP.
- Not allowed / AP not recognized.
- Invalid parameters (e.g. Incorrect MS-ISDN, MS-ISDN, Enduser not registered for mobile signature).
- Unknown parameters.
- Unknown (something failed in the process but we do not know what).

MSSP SigRESP towards AP

- Format (to be defined in Task 2).

- Use of existing standards where they exist is encouraged.

MSSP always provides response to requesting party

- Yes/Successful - proceed (in accordance with MSSP agreement).
- Partial (with reason code, except emergency) - proceed at own risk.
- No/Unsuccessful (with reason code, except emergency) - deny.
- Unable - not confirmed (includes "retry statement").

MSSP and AP may be required to provide positive feedback to Enduser.

All of the above message formats, protocols and error codes etc form part of Task 2 activities.

10.4.2 By the Citizen End-User

Definition of the enduser experience when using his/her mobile device is outside the scope of this activity. However, the "security user experience" shall inform identification of Security Levels in clause 12.3 and form the central activity of Task 3 of this STF.

In addition, the following guiding principles are offered and illustrated in appendix B.

The following conditions may exist in relation to the use of mobile signature "signing" functionality:

- Enduser has completed the mobile signature acquisition process, is in possession of the registered mobile device, a "Signing-PIN" and a signing application on the smartcard.
- Enduser is using a dependent application or service for which mobile signature "signing" functionality and citizen identity is recognized and accepted by the application provider (AP).
- The Enduser is aware (and reminded periodically) of his/her responsibilities and obligations concerning the use of mobile signature "signing" functionality. This includes awareness of the consequences of using mobile signature "signing" functionality to confirm his/her intention to proceed with a transaction (details of which were presented to the Enduser's mobile device and "signed").
- The service type (or application) requires the Enduser to provide his/her mobile signature as the mechanism by which s/he confirms his/her intention for a transaction instruction to be actioned.
- The Enduser shall be presented with positive confirmation on his/her mobile device that something is happening at all times.
- A mobile signature request received at the Enduser's mobile device shall be displayed automatically (i.e. without Enduser intervention) on the mobile device screen.
- The Enduser may be provided with an option to change his/her "Signing-PIN' code at the mobile device.
- The Enduser enters Signing-PIN (Note: at least four digits) via mobile device keypad and selects "OK" to confirm his/her intention to proceed and confirm the transaction instruction received.
- The Enduser should be made aware that it really is a mobile signature application that s/he is launching.
- Each keypad stroke may be represented in the mobile device display screen as a symbol unrelated to the actual key pressed.
- The following Signing-PIN entry and signature response conditions are proposed:

  - No PIN-Entry

    In the case where the citizen does not enter his/her Signing-PIN in the permitted time (i.e. Timeout Limit Exceeded), an appropriate message shall be displayed at the mobile device. In this case a "Time-Out" -type response may be returned to the application provider.

- Incorrect Signing-PIN Entered

  On entry of an incorrect Signing-PIN, an appropriate message shall be displayed at the mobile device indicating that the incorrect PIN has been entered and the number of "re-tries" remaining before the PIN-code is disabled.

- Deliberate Incorrect Signing-PIN entered

  This is an "emergency code" entered by the enduser for any reason. In this case, the signing application may trigger an emergency sequence to advice the application provider not to proceed with the transaction. It may also act to block the Signing-PIN.

- Correct Signing-PIN entered.

  Entry of the correct signing-PIN triggers creation of the citizen's mobile signature which is returned to the application provider by the mobile device via the network operator. Once accepted by an AP, an appropriate status update message will be returned to the Enduser's mobile device and may be displayed automatically. This message may remain on screen until acknowledged by the Enduser.

10.5 Facilitating a Range of Value Added Services

Endusers and APs might elect to take advantage of a range of value added service possibilities, including:

For the Citizen

- Personal Mobile Signature Webpage (for the citizen).
- Signature verification (for the AP).
- Time stamping.
- Electronic transaction receipt storage.

Activation of "signing' functionality at the mobile device may also initiate the creation of a personal webpage for the citizen within the webservice. The webpage may allow the citizen to access records of transactions for which the citizen provided his/her mobile signature (and other services).

The personal webpage might be offered as a "Value Added Service" by the MSSP to enduser citizens. It might also assist with "Customer Service" issues (See later clauses). Access to a personal webpage might itself be controlled by a mobile signature enabled application and may include information and facilities such as:

- A transaction reference number.
- Transaction Details (e.g. Date and Time of transaction, name of application provider, transaction description, etc.).
- A messaging function for communication with the MSSP's customer service operation.
- A facility to prompt the enduser to change his/her mobile signature Signing-PIN periodically.
- an application on the handset.
- Promotional messages for new applications/services that can be used in conjunction with the enduser's existing mobile signature capability.
- Links to other sites managed by the MSSP and/or partners of that MSSP or associated mobile network operator.

10.6 Mobile Signature Lifecycle Management

Once a citizen has acquired mobile signature capability, its continued use requires management. This may involve:

- Replacement/update of mobile signature equipment: smartcard

  smartcards may be updated and/or replaced from time-to-time by the card-issuer for a variety of reasons. In cases where the smartcard is replaced, it may be necessary for the citizen to re-acquire mobile signature capability (including re-establishment of security profiles).

- Replacement/update of mobile signature equipment: Mobile Devices

  Mobile devices may be updated and/or replaced from time-to-time by any entity (including enduser, card-issuer, mobile network operator, application providers and device manufacturers) for variety of reasons. In these cases, it is imperative to ensure that mobile signature capability continues to function in the same (or largely similar) manner as before. Occasionally, this may not be possible and, it may be necessary for the citizen to re-acquire mobile signature capability (including re-establishment of security profiles).

- Update of security profile(s)

  Security profiles, keys and associated certificates may be created with a defined validity period. On expiry of this period, a new profile is required to be created. Alternatively, changes of some attributes forming the security profile (e.g. the citizen's address) may allow the profile to be updated/re-issued, whilst others will require a new profile to be created.

- PIN-code management

  PIN-codes can be blocked, unblocked and/or changed. Blocking may result from incorrect use of the PIN-code (e.g. retry number exceeded, emergency code activated) and may be unblocked by obtaining an unblock code from the card-issuer. Changing a PIN-code may involve issuing a new PIN-mailing, or more likely be performed by the citizen through the mobile device.

- Revocation

  Termination of the mobile signature capability and propagation of termination information throughout the system so that no more signatures can be generated by the terminated device. Revocation may be stem from expiry or be result from misuse of the mobile signature device or by the detection of fraud (or other factors contrary to the term of use).

10.7 Facilitating Customer Service

Information captured and stored in relation to a citizen's security profile and mobile signature may be accessible by a MSSPs customer service agents, subject to the following conditions:

- Issues relating to Data Protection and Privacy are satisfied.
- The "Signing-PIN" is not requested by a customer service agent during any service session.
- The "Signing-PIN" is not revealed by the citizen during any service session.

10.8 Key Factors for Mobile Signature Service Success

The availability of "dependent" applications and the recognition/acceptance of a mobile signature by APs who rely on the signature are key to the success of any mobile signature service. Other success factors include:

- Adoption/service uptake by Endusers.
- Concerns over liability in transactions.
- Ease of use for all stakeholders.
- The mobile signature "result" is considered evidential.

- Service Modularity (e.g. layer model in which security, application and, communications mechanisms/protocols are interchangeable).
- Coexistence of different mobile signature solutions.
- Acceptable revenue sharing arrangements between all stakeholders.

11 Mobile Signature Implementation Challenges

Implementation challenges for mobile signature revolve around the adoption of "portal" strategies by many mobile operators. This effectively requires applications developers and other service providers to realize solutions using different applications Programming Interfaces (APIs). For mobile signature, this has consequences in both the registration and usage phases.

11.1 Mobile Signature Registration

In the internet world, Certification Authorities (CAs) already certify end-users so that they can access application providers on the web. For mobile signature implementations that leverage the use of a mobile device as a smartcard reader, the RA is required to obtain the cryptographic elements required by the CA from the smartcard issuer (e.g. the mobile operator). This may mean that an RA will encounter as many different implementation environments as there are smartcard issuers (e.g. mobile network operators).

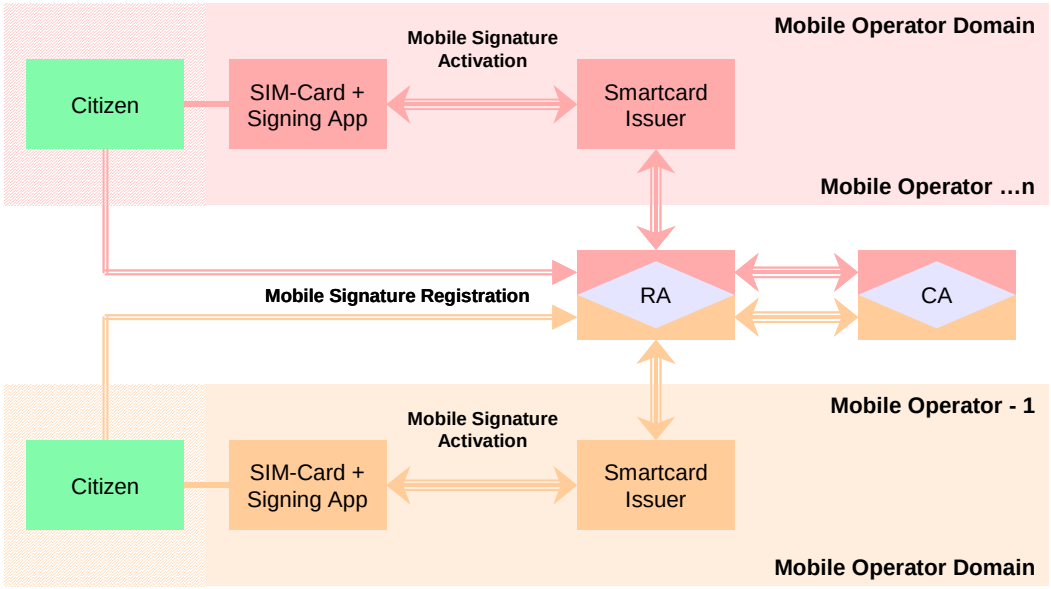


Figure 5: Multiple Registration Environments

Such a situation is too complex for RAs and CAs and a simplified interface to the mobile environment is required. By reducing this complexity for RAs and CAs, citizens requiring mobile signature capability may able to have their personal information and public key certified by **any** CA. In order to achieve this, the following architecture is proposed, making use of a webservice:

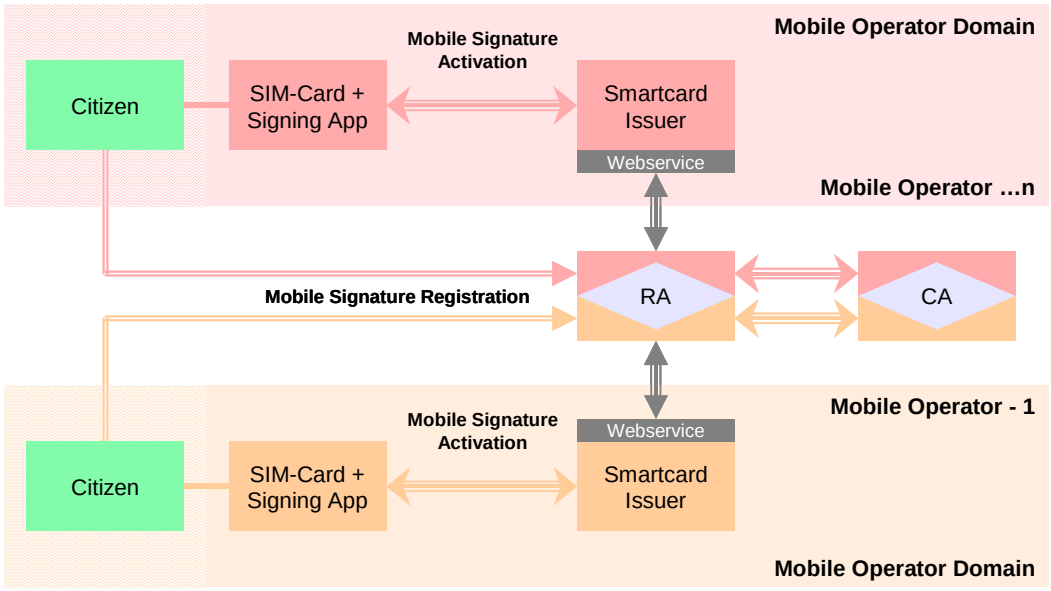


Figure 6: Simplified Registration Interface

Such an approach may not only simplify administration and management issues for RAs and CAs, it would also assist Application Providers (APs) who may be aligned with different CAs. Facilitating the participation of more APs is also likely to widen the choice of applications available to citizens.

11.2 Mobile Signature Usage

In the current mobile environment, a logical implementation of a mobile signature enabled use case requires a bespoke solution, typically satisfying the requirements of a mobile operator's "portal":

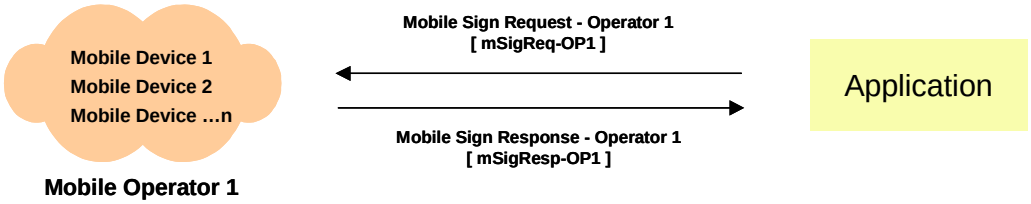


Figure 7: Single Operator Implementation

Whilst it may be attractive for an operator to provide such a "portal" facility for its subscribers, this is limiting for the Application Provider (AP). The AP is either restricted to offering a service to the customers of one mobile network or needing to implement multiple variations of the solution for each mobile network s/he wishes to address. Either way, the financial attractiveness of providing the service is likely to be impacted negatively - sometimes to the point where a service idea may never leave the design stage… and sometimes where pricing issues may defeat service uptake by endusers.

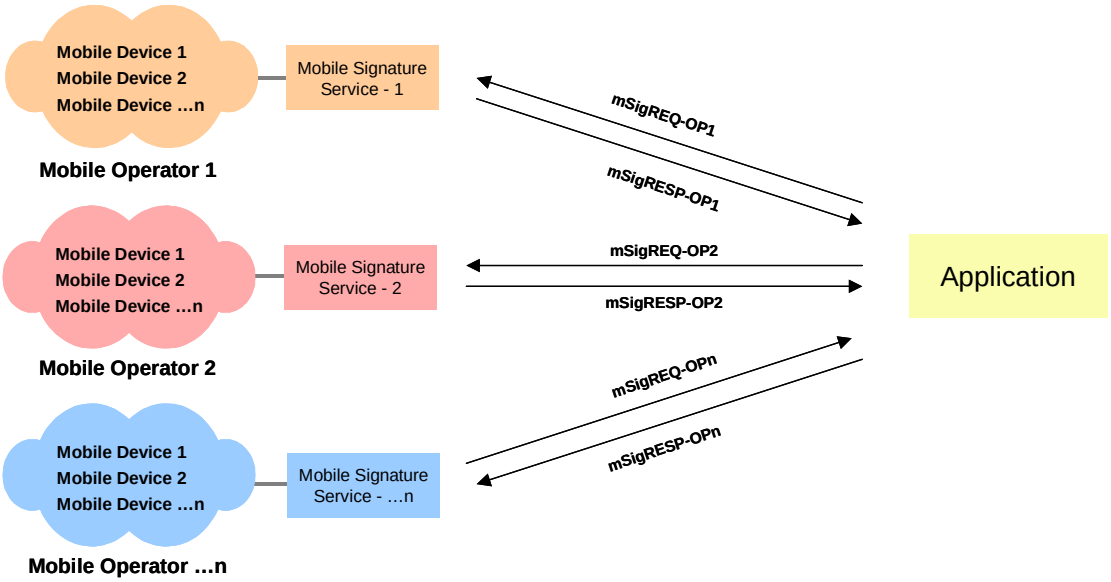


Figure 8: Multi-Operator Implementation

An alternative approach may be to design an intermediary facility with a defined interface to the mobile community for mobile signature enabled applications. This facility (the mobile signature service) might translate standard mobile signature requests from APs into operator-specific commands inside the mobile environment and process appropriate responses accordingly.

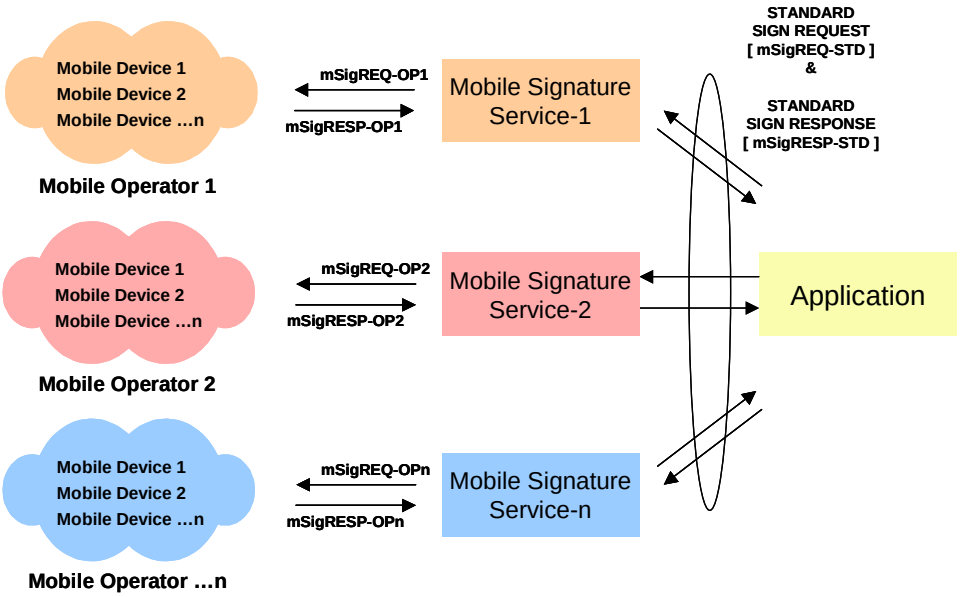


Figure 9: Simplified Multi-Operator Implementation

Whilst such an approach might address cost issues associated with technology, it may also leave commercial considerations unresolved. The AP may still be faced with the administrative cost burden of negotiating commercial terms with as many operators as s/he wishes to address. Even if an AP was able to agree terms with a single operator who maintained commercial relationships with many other operators (e.g. the larger carrier groups) the administrative burden is merely moved from the AP to the operator. This is likely to prove as involved to operators as it is currently to APs.

This situation might be resolved, however, if individual mobile operator webservices were themselves interconnected through another webservice (e.g. a "Roaming Mobile Signature Service"), itself using the "standard" interface. In addition to simplifying matters considerably for the AP, this approach might also address issues of interoperability between operators in a single country or, indeed, operators in different countries.

An interoperable solution also provides the widest addressable mobile user community for APs and, as such, may stimulate applications development.

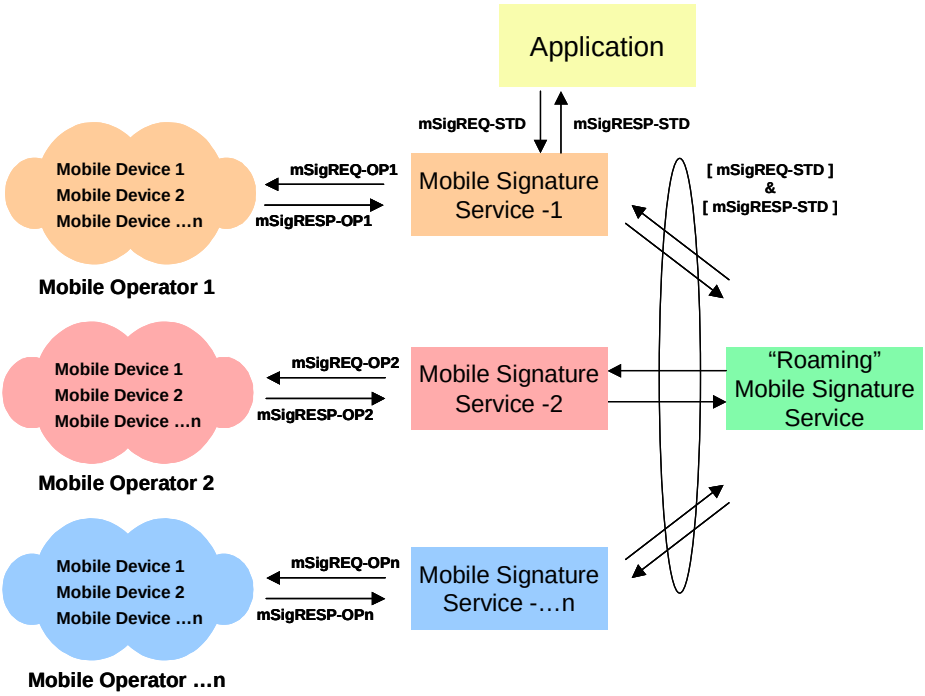


Figure 10: Possible Implementation for Interoperability

In this context, APs are effectively making use of the mobile signature services provided by each operator as part of an industry-wide solution. Such a service might be governed by a single set of contractual terms and conditions (Note: subject to local variations), as is the case with mobile voice telephony under the guidance of the GSM Association (GSM-A).

A discussion of the roles and responsibilities for realizing mobile signature service implementations is provided in clause 12.

12 Potential Roles and Responsibilities

The clause describes the roles identified in the mobile signature process and responsibilities of the entities that might be involved. Roles are described in relation to which entity may be best placed to undertake a particular role.

12.1 Roles

It is clear from the description of mobile signature service registration and usage provided above, that the following roles can be identified:

- Enduser.
- Smartcard Issuer (e.g. Mobile Network Operator).
- Registration Authority (RA).
- Certification Authority (CA).
- Mobile Signature Service Provider (MSSP).
- Application Provider (AP).
- "Roaming MSSP".

- Contractual Management Co-ordinator (e.g. GSM Association).

In the first iteration, the MSSP role might most obviously be provided by the Smartcard Issuer (e.g. the mobile network operator). It may be possible for other organizations to undertake the role of MSSP, however, but this may require a contractual arrangement with a mobile network operator. In effect, is because the mobile operator already owns primary responsibility for managing all issues relating to the smartcard (e.g. the SIM-card) for provision of the core GSM telephony services. Indeed, some of the information managed by the operator is required by the RA and CA in order to facilitate the mobile signature certification process for the RA and CA:

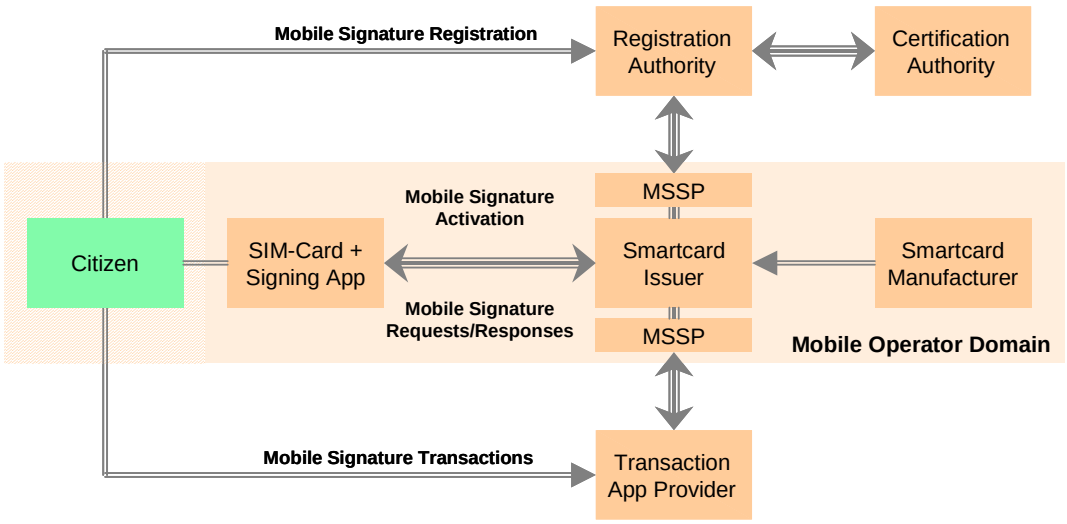


Figure 11: Mobile Signature Roles

The RA and CA roles might also be provided by the network operator, particularly in the case of the larger carrier groups where investment costs may be amortized across the group companies. Alternatively, these roles might be outsourced by network operators to specialist providers for business case and management reasons.

In the case of the Application Provider (AP) role, different considerations may apply and a network operator is likely to be just one of many APs offering services to citizens forming the network subscriber base. This is because the amount of effort needed to design, develop and manage the product portfolio lifecycle may be greater than that which can be achieved by the operator alone. In this respect, the NTT DoCoMo i-Mode model is of interest, where an AP community works in a shared revenue partnership arrangement with the network operator in order to maintain a **compelling** application/services portfolio for the subscriber base.

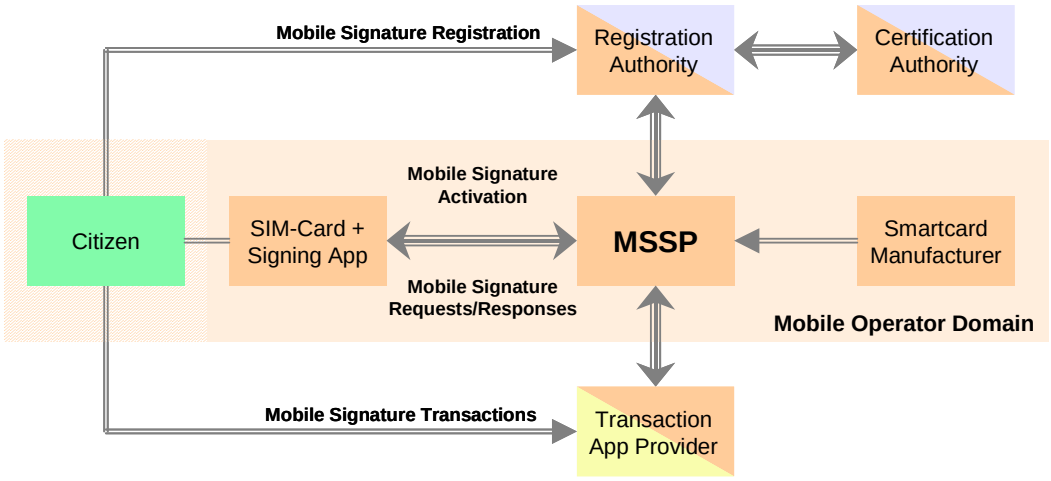


Figure 12: Pivotal Role of MSSP

Placing the MSSP at the centre of the mobile signature commercial model may also facilitate "Transaction Roaming". This is a concept in which a subscriber of one mobile network accesses the portal of another operator in order to use an application/service, either in the "home" territory or when "roaming" (see GSM voice roaming). In transaction roaming, however, liability for the transaction should reside with the citizen rather than his/her "home" network, as is the case with voice roaming through the terms of roaming agreements.

When a citizen uses an application/service in the visited network, the AP aligned with that network, issues a signature request to his/her MSSP in the usual way. The signature request may be forwarded to the citizen's "home" MSSP for communication with a citizen's mobile device and, perhaps more importantly, for verification that the returned mobile signature is valid. In this respect, the visited network is effectively acting as an "acquiring" network for the citizen's home - or issuing - network.

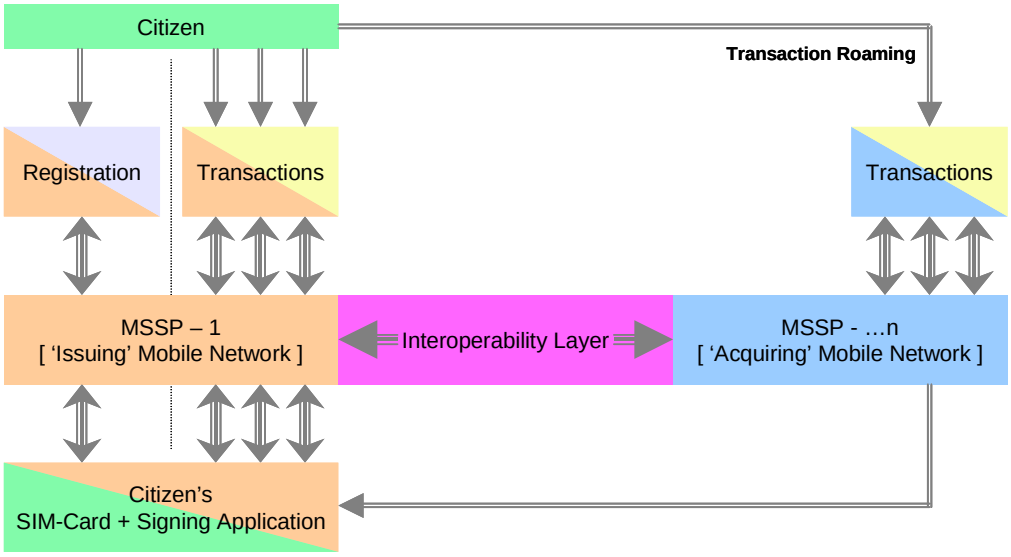


Figure 13: Transaction Roaming

Issues relating to "Interoperability" for transaction roaming are considered in Task 4 of the STF.

However, it may be appropriate that the interoperability function ("Roaming-MSSP") is provided by a separate entity. In this case, it may be preferable that a separate organization be formed which is funded and owned collectively by the network operators and those parties who choose to rely on mobile signature for whatever reason. An illustration of just one of many commercial model possibilities is offered for consideration by other groups, such as that managing the "T2R" project (IST-2001-38632), also funded by the EC.

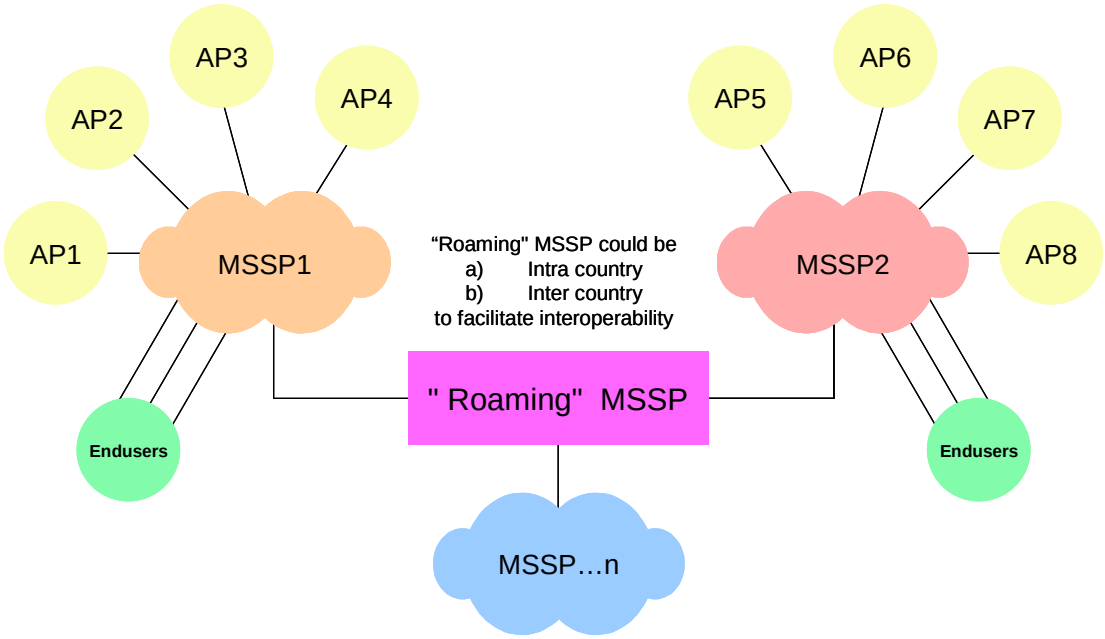


Figure 14: Sample Commercial Model for MSSP Interoperability

12.2 Responsibilities

Each of the roles identified will have particular responsibilities and these may be governed by commercial agreements between the parties. These are likely to include considerations of the "quality of service" provided by each party to the others and, of course, matters relating to "security".

12.2.1 Enduser/Citizen

The enduser/citizen is responsible for providing authentic personal information during the registration phase and for the consequences of every transaction authorized when using his/her mobile signature.

12.2.2 Smartcard Issuer / Mobile Network Operator (MNO)

The smartcard issuer is responsible for providing information to the RA that allows completion of the mobile signature registration phase and for activating the signing application where smartcards are supplied to end-users with this application in a pre-active (i.e. Dormant) state.

Basically, the Mobile Network Operator is responsible for the operation of the core mobile telephony service (including roaming aspects). However, in the case where the smartcard issuer is the Mobile Network Operator, the MNO is responsible for all maters relating to the GSM smartcard (SIM-Card), including the signature application and generation of the cryptographic elements (either in the card production or onboard the card itself).

12.2.3 Registration Authority (RA)

The RA is responsible for acquiring and validating personal information provided by citizens wishing to use the mobile signature service. This responsibility will be discharged in accordance with a particular CA's policy (i.e. certificate policy and certification practice statement) and includes obtaining "proof-of-possession" of a citizen's private key/public key pair and the identity of the public key itself.

12.2.4 Certification Authority (CA)

The CA is responsible for processing information from the RA and certifying the public keys of citizens who wish to use the mobile signature service. In addition, the CA will provide a certificate revocation service (i.e. to manage mobile signature lifecycle and permit audit transaction investigations). Security is a primary responsibility for the CA, such that application providers may rely of the authenticity of a citizen's mobile signature.

12.2.5 Mobile Signature Service Provider (MSSP)

The MSSP may be responsible for the quality-of-service of the core mobile signature service (i.e. processing of signature requests to acquire mobile signatures from citizens). Elements contributing to "quality-of-service" might include:

- The degree of confidence.
- System loading.
- Platform processing capacity.
- Peak load performance.

This might be enhanced through the provision of added-value services intended to assist relying parties and citizens alike, including "signature verification", "time stamping" and notarization, etc.

12.2.6 Application Provider

Application providers are responsible for providing "dependent" applications/services that citizens may use. APs should design applications in conjunction with the smartcard issuer to ensure that the user experience of the "signing" act is consistent with other applications/services from other providers used by a citizen.

12.2.7 Roaming-MSSP

The Roaming-MSSP is responsible for all matters relating to interoperability of mobile signature services between different MSSPs.

12.2.8 Contractual Management Co-ordinator

The Co-ordinator may be a sub-role for one of the other roles identified. The purpose of this role is to facilitate interoperability of mobile signature services from a contractual perspective. In many respects, the responsibilities envisaged are similar to that currently managed by the GSM Association for voice roaming services (i.e. drafting of a standard, industry-wide set of terms and conditions used by mobile network operators to inform their commercial negotiations).

12.3 Security Provisions

NOTE: Task 3 of the Mobile Signature STF is concerned with the definition of security levels for mobile signature services and the security user experience for any security levels identified.

12.3.1 Security Levels

The EU Directive defines two level of electronic signature (i.e. Electronic and Advanced Electronic). The STF activity may produce gradations of the EC definition for "Electronic Signature", but must ensure that any new elements introduced for mobile signature are "safe" in relation to the existing definition for "Advanced Electronic Signature".

From the European Directive, EESSI/ISSS E-SIGN Workshop has defined the following "security levels".

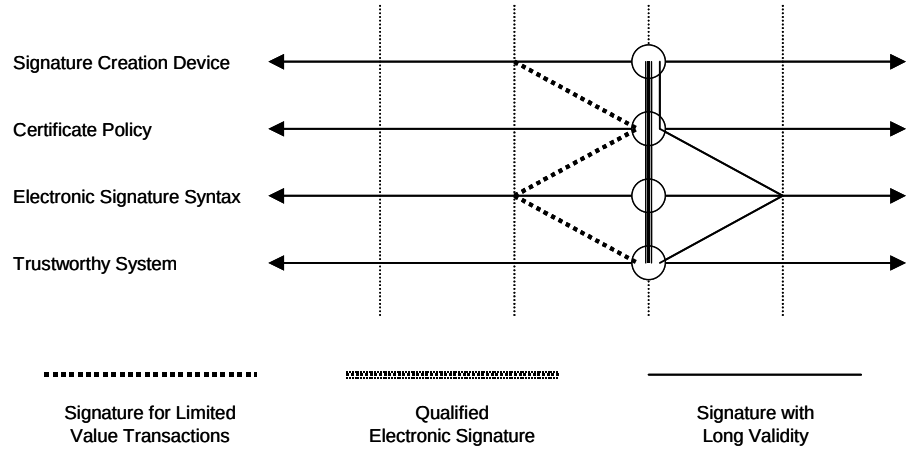


Figure 15: Security/Quality Levels

Wherever possible, the STF will make use of previous standardization efforts, including:

- European Electronic Signature Standardization Initiative (EESSI) work on Enhanced Electronic Signature.
- US Department of Commerce Federal Information Processing Standards (FIPS).

This may extend to making use of definitions and conventions adopted by these organizations.

12.3.2 General Principles for End-User Security Experience

In all respects, it is imperative that the user experience is consistent, irrespective of the application which generates a mobile signature request. Mobile signature requests shall contain sufficient information to allow determination by the citizen whether s/he wishes to proceed with a transaction presented at his/her mobile device screen (i.e. "What-you-see-is-what-you-sign").

Entry of the Signing-PIN by the citizen may be represented on screen by characters which bear no resemblance to the actual keys pressed by the citizen. Once the mobile signature has been processed, the citizen may be provided with positive confirmation of the outcome (i.e. success/fail).

12.3.3 MSSPs

MSSPs are responsible for the service facilities they provide. MSSPs may be required to demonstrate compliance to contractual agreements (where they exist), including active management of:

- Prepare a documented security policy.
- Prevent Unauthorized Access to databases, etc.
- Detect Unauthorized Access to databases, etc.
- Processes to monitor vulnerabilities.
- Actual monitoring for system vulnerabilities.
- Record and retain system information sufficient to perform security audits and investigations.
- Record and retain security audit reports.

MSSPs may also be responsible for physical elements used in the delivery of services they provide (e.g. mobile equipment). This might include (but not be limited to) the following elements:

- Provide assurance that "what the user sees is what the user signs…".
- The PIN should be erased from all memory after being transmitted to the card.
- A card with which no interaction occurring should be powered off after a prescribed time-out.

- No application capable of mimicking the screens of appendix B should be installable in the mobile handset.
- No application capable of disclosing the PIN (e.g. Capturing it and sending it via SMS) should be installable in the mobile handset.
- The keying of the PIN should not generate DTMF signals (a malicious party eavesdropping the communication could then determine the PIN that way even if the PIN itself is not transmitted out of the mobile handset!).
- Users may have the ability to customize the screens displayed by the mobile handset (the goal being to avoid confusing the user with a fake mobile handset whose sole function is to capture the PIN).
- The signature and the signed message should be erased from all memory after use.
- The keying of the PIN may result in the display of a sequence of characters unrelated to the PIN's value of length.
- The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
- All software running on the ME should be immune to buffer overrun attacks.
- Citizens may have the ability to terminate the mobile signature service from the mobile device (e.g. in emergency/distress situations).

12.3.4 Application Providers

Application Providers are responsible for the security of the applications that leverage the mobile signature. APs must provide the assurance that the signed data is relevant from an application security standpoint.

Typically, in a purchase transaction, the user must sign the product's reference and price. Omitting the price from the signed message makes repudiation possible and disqualifies the signatures as a non-ambiguous proof of the user's intention to pay a given price.

It is the APs responsibility to ascertain that the complete set of data elements needed for the application's security is indeed signed.

12.3.5 Smart-Card Issuers

- Provide assurance that "what the user sees is what the user signs…".
- The signature algorithm and the PIN verification routine running on board should be immune to timing attacks.
- The signature algorithm and the PIN verification routine running on board should be immune to power and electromagnetic side channel attacks.
- The signature algorithm and the PIN verification routine running on board should be immune to fault attacks.
- The secret material (PIN, signature key) stored in the card should be immune to invasive attacks and external observation techniques (e.g. Electronic Scanning Microscope).
- A citizen's Signing-PIN should consist of at least four digits, as determined by "normal" risk management practices.
- The PIN verification routine should be protected by a ratification counter. The limit of this counter will be determined at a later step.
- PIN management routines should allow the user to change his PIN if he wishes so.
- The signature key should not be derived from the PIN without the adding of extra entropy.
- The random number generator used for generating the card's signature should resist physical modification attempts.

- The random number generator used for generating the card's signature should satisfy randomness tests that will be specified later (we recommend Maurer's universal test and Diehard randomness test battery).
- Signature cards should have an auto-destroy function. A transaction should always begin by the card querying a signature from the server of a nonce generated by the card and completed with a seemingly random nonce added by the server. If the server signs a specific nonce the card will erase from its EEPROM its PIN and signature key.
- The PUK will have a ratification counter.
- The card will count the number of signatures generated with each PIN and as this number exceeds a pre-determined limit will ask the user to change his PIN.
- The card will associate to each PIN a creation date. At the beginning of each transaction the card will receive a signed message specifying the current date. If this date is inferior that the previously recorded date in the card the card will block itself, if this date is superior the card will update its date. If the card exceeds a given date the card will ask the user to modify the PIN.
- The card could have two modes: a long PIN mode and a standard PIN mode. Their use is as follows: the card will ask the user to present a long PIN once each n signatures. In case of theft, a thief who was able to guess the user's standard PIN could generate at most n-1 signatures.
- When a PIN is replaced the two past PIN values can not be reused.
- All combinations of commands accepted by the card's command dispatcher should not cause internal state security inconsistencies.
- All software running on the card should be immune to buffer overrun attacks.
- A mobile signature issued by the card should be issued with a defined validity period.

13 Interactions and Interfaces

This clause outlines the basic-level interactions and interfaces between the different roles that may be required to realize mobile signature solutions. Descriptions are offered for the registration phase and for transactions in both the "home" (i.e. "issuing") and "visited" (i.e. "acquiring") networks as the starting point for Task 2 of the ETSI STF. These descriptions are provided for just one potential in each activity.

13.1 Overall Architecture

The overall architecture is shown below. This illustrates citizens of different smartcard issuers registering for the mobile signature service and using their mobile signature capability, in the "home" (or "issuing"). An interoperability layer may allow "Transaction Roaming".

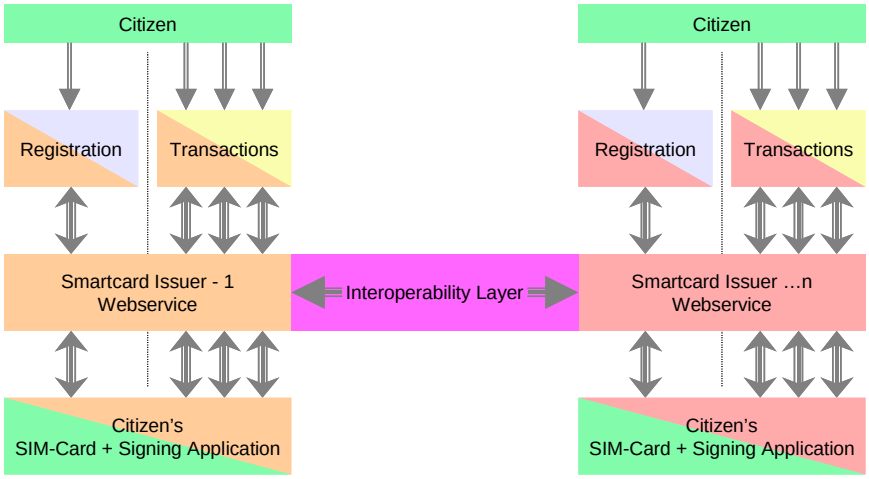


Figure 16: Overall Architecture

13.2 Interfaces between Entities

Interfaces exist between entities exist throughout the mobile signature process to facilitate initial citizen registration and, of course, mobile signature usage.

13.2.1 Registration and Certification

Four entities are involved in a mobile PKI registration process; End-user, MSSP, Registration Authority (RA), and Certification Authority (CA). The diagram illustrates the interaction between these entities (Note: a MSSP may own RA and CA entities or outsource these to specialist providers).

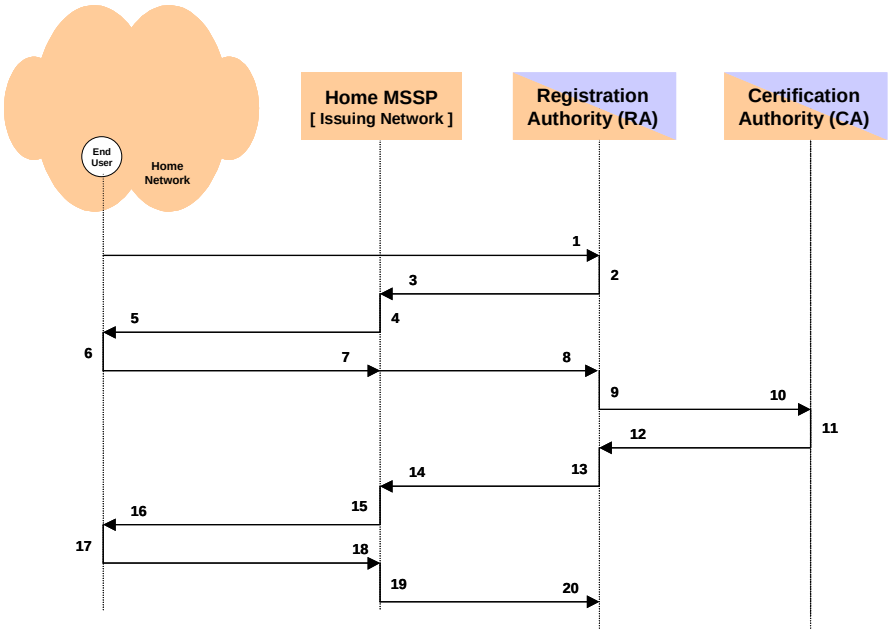


Figure 17: Registration and Certification Phase

The process steps are described below:

1) Enduser - confirms registration to a Registration Authority and provides the RA with appropriate personal information (e.g. MSISDN, Name, M).

2) RA - Process enduser's confirmation; initiate data …

3) RA - Proof Of Possession request to MSSP.

4) MSSP - looks for end-user entry in its customers' database; if the end-user is a MSSP's customer: either a predefined (server-side solution or a POP computed at the SIM card personalization phase) POP is known and responded to the RA or the MSSP uses a bespoke solution in order to get one from the end-user. If the end-user is not a MSSP's customer, an error code is returned.

5) MSSP - POP mobile signature request (bespoke).

6) End-user - POP is computed by the SIM Card.

7) MSSP - POP mobile signature response (bespoke).

8) MSSP - POP response to RA.

9) RA - prepares a certification request thanks to the POP and the end-user credentials.

10) RA - certification request to the CA.

11) CA- issues the end-user certificate.

12) CA - certification response containing the end-user certificate.

13) RA - processes response from CA.

14) RA - certificate download request to MSSP.

15) MSSP - prepares a Certificate download request.

16) MSSP - certificate download request.

17) End-user - end-user's certificate or a certificate identifier is stored on the end-user's mobile handset.

18) End-user - acknowledgement.

19) MSSP - updates end-user's profile.

20) MSSP - acknowledgement.

13.2.2 Home Network Transactions

Where a citizen is located in his "home" network coverage area and using a dependent application from an AP aligned with that network operator, transactions are likely to be completed as follows.

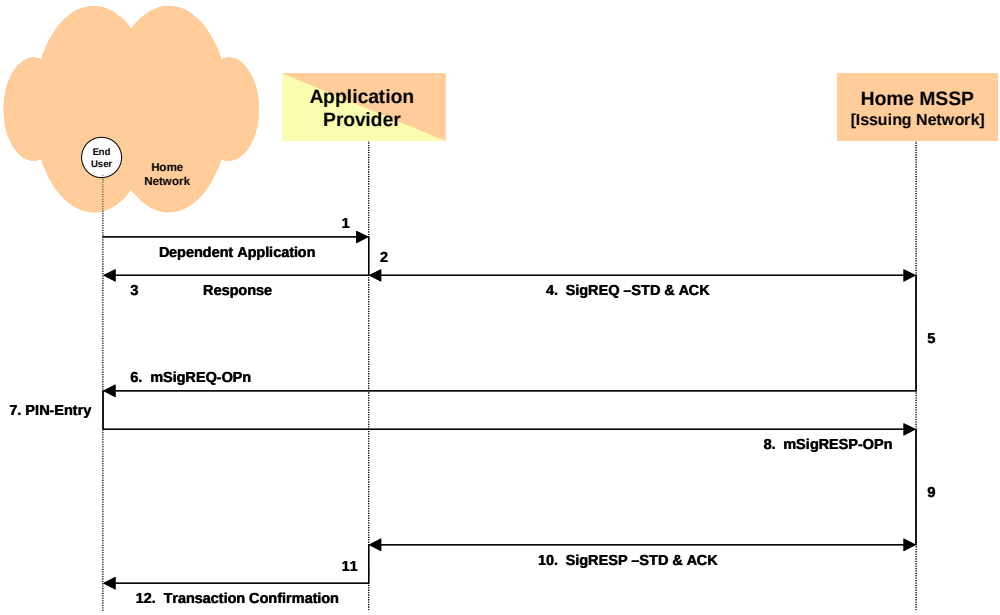


Figure 18: Home Network Transactions

The process steps are described below:

1) Enduser - confirm a transaction or wants to access a service.

2) AP - Process enduser's confirmation; initiate data …

3) AP - informs the enduser via the applications channel (e.g. Internet) that he is going to invoke his mobile signature application in order to confirm the transaction.

4) AP - Standard signature request (SigREQ-STD) to Home-MSSP.

5) Home-MSSP - Process SigREQ-STD from AP; Evaluate best Sign-acquisition route.

6) Home-MSSP - mSig request to Enduser.

7) Enduser - the mobile handset displays the text to be signed etc. (see enduser experience) and (the SIM card of case of GSM) computes a digital signature following PIN-entry by the citizen.

8) Mobile device returns mobile signature response to the Issuing-MSSP.

9) Home-MSSP processes the signature response (including any value added service elements such as secure storage of the signature receipt; signature validation; timestamping, etc.).

10) Home-MSSP transmits the signature response back to AP (along with a mobile signature confirmation to the end users mobile device - Optional).

11) AP prepares acknowledgement for the citizen.

12) AP confirms result of mobile signature process and status of the transaction (e.g. completed, failed - with reason code, etc.).

13.2.3 Transaction Roaming

In situations where a citizen is located in coverage area of a "visited" network and is using a dependent application aligned with that network operator, transactions may be completed according to the following scheme.

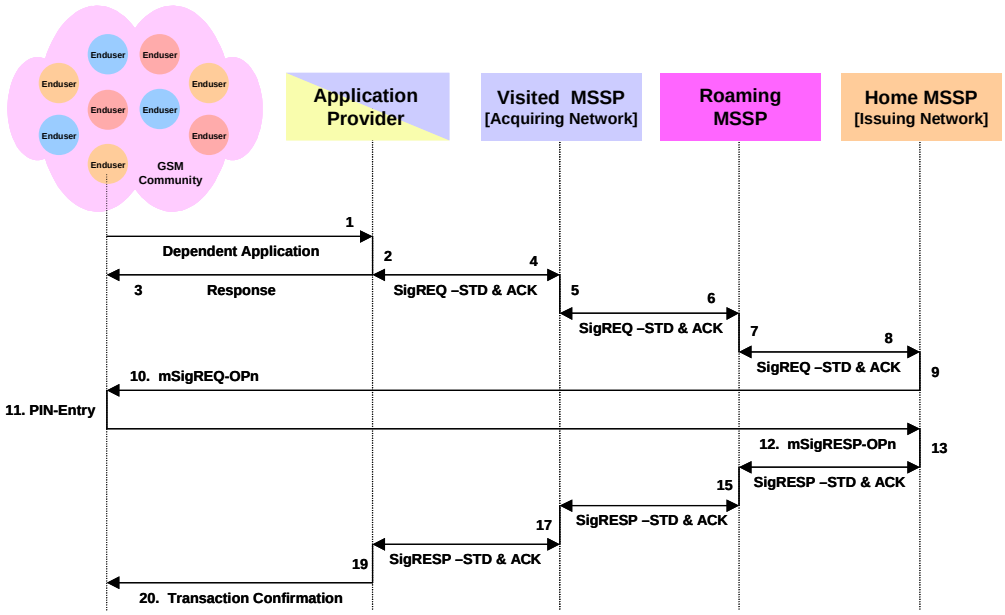


Figure 19: Transaction Roaming

The process steps are described below:

1) Enduser - confirm a transaction or wants to access a service.

2) AP - Process enduser's confirmation; initiate data …

3) AP - informs the enduser via the applications channel (e.g. Internet) that he is going to invoke his mobile signature application in order to confirm the transaction.

4) AP - sign request to his/her MSSP.

5) MSSP identifies that the citizen is a subscriber of another network.

6) MSSP in his/her role as "acquiring" network forwards the signature request to a Roaming-MSSP.

7) Roaming-MSSP identifies the citizens "home" MSSP and "issuing" Network.

8) Roaming-MSSP forwards signature request to "home" MSSP.

9) Home-MSSP processing signature request.

10) Home-MSSP forwards mobile signature request to citizen's mobile device.

11) Enduser - the mobile handset displays the text to be signed etc. (see enduser experience) and (the SIM card of case of GSM) computes a digital signature following PIN-entry by the citizen.

12) Mobile device returns mobile signature response to the Home-MSSP.

13) Home-MSSP processes the signature response (including any value added service elements such as secure storage of the signature receipt; signature validation; timestamping, etc.).

14-18) The signature response is transmitted back to AP.

19) AP prepares acknowledgement for the citizen.

20) AP confirms result of mobile signature process and status of the transaction (e.g. completed, failed - with reason code,, etc.).

13.2.4 Other Possibilities

Clearly, many other possibilities for transaction roaming exist. For example, the citizen might be located in the coverage area of his "home" network operator but using an application operated by an AP aligned with another network. This scenario is not illustrated here, but may follow a similar process as described above.

13.2.5 Interfaces between entities

The following table captures the interfaces between the various entities.

Table 2: Interfaces between entities

Party 1	Party 2	Interaction
End user	RA	• Registration
RA	MSSP	• Proof-of-Possession
RA	CA	• Certification request
MSSP	End user	• PIN mailer
AP	MSSP	• Registration • Activate mobile signature service • Mobile signature: Signature Request and Response • Query on mobile signature status • Query end user's proof of possession of the signing key • Update mobile signature details • Verification of a mobile signature

Party 1	Party 2	Interaction
MSSP operator	MSSP	• Query on mobile signature status • Update mobile signature details • Request to suspend mobile signature service • Change personal information • Change ASP's profile • Service configuration
Customer Care	MSSP	• Query on mobile signature details • Update mobile signature details • Activate mobile signature service • Suspend mobile signature service • PIN Code Management • Request to reissue PUK number

All these interfaces are subject to interoperability concerns and are specified/standardized in Task 2 as functions exported by a web service. APs can access them as enablers for the service they provide. The MSSP operator and the customer care entity can access them in order to manage the mobile signature service. The customer care entity and the MSSP operator may engineer a web portal that calls the interfaces listed above.

13.2.6 Applicable/Available Standards

The solution should be based on open standard protocols and technologies and deliver a set of open specifications that can be implemented on a range of platforms, wherever these are available and are appropriate for the limitations of mobile devices.

The present document will rely as much as mobile applicative constraints allow on existing standards and formats, possibly adapted and modified.

14 Requirements

14.1 Business Requirements

Requirement	Category	Mandatory Recommend Optional	Comments
In promotional materials, the concepts of mobile signature and mobile signature service should be described in non-technical, layman terms.	General	R	
The mobile signature service should provide information in a clear and unambiguous manner.	General	R	
Mobile signature provides the ability for a citizen to authorize a transaction instruction.	General	M	
Mobile signature provides the opportunity for third parties to acquire a citizen's permission to proceed with a transaction.	General	M	
Mobile signature is an enabling technology for electronic commerce.	General	R	
Mobile signature service should leverage web technology, wherever possible.	General	R	
Mobile signature service should make use of existing standards wherever they exist (e.g. PKCS#…) and are appropriate for the limitations of mobile devices.	General	R	Any existing standards used should also be specifically appropriate for the technical and commercial requirements of the mobile signature service.
Mobile signature should leverage core mobile network infrastructure, mobile device technology (including SIM-card) and customer service facilities wherever possible.	General	R	

Requirement	Category	Mandatory Recommend Optional	Comments
Mobile signature services should be implemented using a modular (layer) approach, separating application layer, from security layer, from network bearer layer.	General	R	
The cryptography choice is a matter for MSSPs.	General	O	
Application providers shall use a standard message format to issue mobile signature requests to MSSPs.	General	M	
MSSPs shall use a standard message format to issue mobile signature responses to application providers.	General	M	
MSSPs shall use standard message formats to issue mobile signature requests and responses to other MSSPs.	General	M	
MSSPs may use standardized network communications bearer technology and interfaces when communicating with mobile devices in their own network community.	General	O	
The core mobile signature service is to acquire a mobile signature from a citizen on behalf of an application provider.	General	M	
The mobile signature service shall be capable of facilitating the mobile signature process.	General	M	
MSSP may provide a "test" application to allow citizens to gain experience of mobile signature usage.	General	O	
Citizens may be provided with a transaction receipt for each mobile signature transaction.	General	R	
Citizens should be able to provide their mobile signature to applications providers associated with visited mobile networks where the mobile signature service is recognized and accepted.	General	R	

Requirement	Category	Mandatory Recommend Optional	Comments
Mobile signature service specified by ETSI does not infringe intellectual property rights (IPR) of any third party.	Legal	M	
All IPR licences, where required, are obtained under ETSI standard policy guidelines.	Legal	M	
Mobile signature service providers should comply with local law enforcement requests (subject to due process, etc.).	Legal	R	
All entities involved in the provision of mobile signature services must resolve a common approach to liability, particularly in relation to legal responsibility for security and quality of service.	Legal	M	
MSSPs shall be accredited by…	*LEGAL*	*M*	***COMMENTS WELCOMED***
Citizen's personal information shall be managed in accordance with Data Protection and Privacy regulations.	Legal	M	
Mobile signature service should promote and facilitate the largest addressable community of citizens (consumers) for the application provider community.	Commercial	R	
Mobile signature service should adopt an architecture promoting interoperability and lowest deployment costs.	Commercial	R	
Mobile signature service should adopt an architecture offering the lowest "per transaction" cost, subject to other prevailing marketing rationale.	Commercial	R	
Mobile signature services should be provided to application providers subject to the terms of a contract (AP and MSSP)	Commercial Legal	R	
MSSP technology choice and quality of service may be described in commercial contracts between MSSPs and APs.	Commercial Legal	O	

Requirement	Category	Mandatory Recommend Optional	Comments
Mobile signature services should be provided to citizens subject to the terms of a contract (citizen and MSSP)	Commercial Legal	R	
It may be possible for an MSSP to offer value added services to their clients (e.g. personal web page, time stamping, signature verification, electronic receipt storage).	Commercial	O	
Mobile signature service may be used by applications providers who are known and registered with an MSSP.	Commercial	O	
The present standard will rely as much as mobile applicative constraints allow on existing standards and formats, possibly adapted and modified.	General	R	
Mobile signature requests from APs and mobile signatures returned by citizens may use mobile network resources which represent "chargeable" opportunities but which may be zero-rated by the mobile network operator.	Commercial Legal	O	
Dispute resolution policy.	Commercial Legal	R	
Mobile signature service registration should "capture" sufficient personal information (i.e. attributes) about the citizen to form an identity that offers a suitable degree of confidence for an application provider.	Registration Legal	M	
During the registration phase, a citizen should be required to prove that s/he is registered user of the mobile device as a pre-condition for activating the signing functionality in a mobile device.	Registration	M	
Citizens' may register for mobile signature service by telephone, via the Internet and by visiting a MSSPs (or an MSSP agent's) retail store.	Registration	O	Internet registration may only be an acceptable method for citizens who are recognized by the MSSP (e.g. maybe from a previous registration that occurred in person) or who can verify their identity using another electronic signature supported by a certificate managed an entity that is recognized (and acceptable) by the MSSP.

Requirement	Category	Mandatory Recommend Optional	Comments
The registration method used by the citizen should form part of the citizen's identity (e.g. remotely registered).	Registration	R	
Mobile signature service user experience should be such as to maximize understanding (i.e. prevent confusion) or to prevent fraudulent or misleading use : "What-you-see-is-what-you-sign".	Experience	R	
Citizens should be provided with positive confirmation of all actions relating to the use of a mobile signature service.	Experience	R	The meaning of this confirmation might be variable and is to be defined by the MSSP or the AP.
A customer should be made aware (and periodically reminded) of the consequences of providing a mobile signature.	Commercial Legal	M	
Citizens should be able to choose their own Signing-PIN and to be encouraged to change this from time-to-time.	Experience	R	
Mobile signature services may be capable of being used to supplement existing application security arrangements or to be used as the primary security mechanism in their own right.	Security	O	
MSSPs shall be audited periodically by…	*Security Legal*	*R*	***COMMENTS WELCOMED***
Mobile signature should permit citizens to provide a way of providing an electronic signature.	Security Legal	R	
Mobile signature service providers shall prepare an appropriate security policy.	Security	M	
Mobile signature service providers shall adopt appropriate security methodologies to prevent and detect unauthorized access to databases.	Security	M	

Requirement	Category	Mandatory Recommend Optional	Comments
Mobile signature service providers shall undertake security monitoring to identify security vulnerabilities and undertake appropriate corrective action where these are identified.	Security	M	
Mobile signature service providers shall retain information sufficient to perform security audits and assist with security investigations.	Security	M	
A mobile signature should be issued with a defined validity period.	Security	R	
Citizens may have the ability to terminate the mobile signature service from the mobile device (e.g. in emergency/distress situations).	Security	O	
A citizen's Signing-PIN should consist of at least four digits, as determined by "normal" risk management practices.	Security	R	
During keypad entry the Signing-PIN should be represented by a symbol unrelated to the actual key pressed.	Security	M	
The citizen's Signing-PIN should be known only to the Citizen.	Security	M	
Customer service agents shall under no circumstances request a citizen to reveal his/her Signing-PIN during customer service calls.	Security	M	
The overall system should implement all appropriate measures to prevent screen masquerade in the signature request text and/or the PIN-entry screen.	Security	M	

14.2 Functional Requirements

Requirement	Process Step	Mandatory Recommended Optional	Comments
A web page published by authorized MSSP in order to describe the service.	Awareness	R	
Web page may be edited by authorized MSSP.	Awareness	R	
Web page that may contain a demonstration of a selection of use-cases.	Awareness	O	
Web page contains full contact information + messaging facility to contact MSSP customer care.	Awareness	R	
Intranet information bank available to MSSP.	Awareness	O	
Entry point is provided in order to proceed with the registration (Web, IVR, Shop, WAP…).	Registration	R	
Registration template (e.g. Web form).	Registration	M	
Collect required end-user's attributes.	Registration	M	
Registration confirmation.	Registration	M	
Create end-user's profile in MSSP's database.	Registration	M	
Update end-user's profile in MSSP's database.	Registration	M	
Replace citizen's SIM-card.	Registration	O	
Activate signing application.	Registration	M	
Citizen must be alerted of arrival of signature request	Use	M	

Requirement	Process Step	Mandatory Recommended Optional	Comments
Way of alerting about the arrival of a signature request might be a beep and/or a visual display,	Use	R	
Key generation (server-side or on-board SIM-card).	Registration	M	
PIN code initialization + mailer.	Registration	O	
Smart-card personalization (Note: may include key generation, PIN code initialization etc.).	Registration	O	
Arrange for (or organize) the creation of any certificates required to support the mobile signature.	Registration	M	
Test application (so that the user is able to practice before making transaction commitment and test the signing functionality from time to time).	Registration	O	
Mobile signature application activation/de-activation.	Registration	R	
Compliancy with ETSI specifications to be assessed/audited by independent entities.	Use	M	
Receive standard signature request (SigREQ-STD) from APs or other third parties (e.g. other MSSP to facilitate transactions roaming).	Use	M	Possible
SigREQ Routing (best acquisition route identified thanks to the end-user's profile).	Use	M	Possible
Obtain mobile signature (Use of various bearers to dialogue with a mobile signature application).	Use	M	
Retry policy.	Use	R	
Mobile signature validation.	Use	R	

Requirement	Process Step	Mandatory Recommended Optional	Comments
Timestamping.	Use	O	
Signature records storage.	Use	O	
Store transaction details: LOG.	Use	O	
End-user Acknowledgement.	Use	M	
Send signature response (SigRESP-STD) to AP or other third parties (e.g. other MSSP to facilitate transactions roaming).	Use	M	
Dispute resolution features.	Use	R	
Protocol atomicity (i.e. in case of "failure" due to malfunction the transaction is recoverable or cancelled in accordance with signing validity period).	Use	O	
AP's profile management.	Cust Svc	R	
PIN code management.	Cust Svc	M	
PUK management.	Cust Svc	M	
Query on transaction details.	Cust Svc	R	
Change transaction details.	Security	O	
Fraud recognition.	Security	M	
Intrusion detection.	Security	M	
Tamper resistance of signing device (i.e. SIM-card).	Security	M	In accordance with mobile network operator's SIM-card policy…

Requirement	Process Step	Mandatory Recommended Optional	Comments
Immunity of signing device (i.e. mobile device + SIM-card) to logical attacks (e.g. buffer over-runs, trojan horse, etc.).	Security	R	

Followed by explanation of features as required…

15 Conclusions

The present document provides guidance for drafting of ETSI Technical Specifications concerning Interfaces, Security Provisions and Interoperability for implementation of industry-wide mobile signature services.

One of the prime goals of the present document being to trigger discussions, it has been decided to add a formal conclusion clause to it once the public review period has ended.

Annex A:
Generic Use Case "Template"

ADVICE for USING the TEMPLATE

- Use cases should be constructed in order to make use of the condition "I agree to this request" provided by the citizen in response to a mobile signature request.
- The mobile signature request needs to describe the essential text to be signed (i.e. the transaction instruction) that will be deemed to be authorized once a citizen provides his/her mobile signature in response to the request.

Because:

- *[a few bullet points that help position the use case]*

USE CASE NAME - tba	
Service Proposition:	TBA
Service Type:	TBA
Market Segment:	TBA
Target Market:	TBA
PRE-CONDITIONS	
Condition:	Description
A	*TBA*
B	Citizen has acquired mobile signature capability.
C	Citizen has registered to use this application.
Description Of Service NOTE: ONLY the "POSITIVE" (i.e. mobile signature successful) condition described.	
Step:	Description
1	*TBA*
2	*TBA*
3	*TBA*
4	*[Application Name]* application prepares *[transaction instruction]* and an associated mobile signature request containing the text to be signed (Note: to be used to authorize the transaction instruction).
5	Mobile signature request received by mobile signature service.
6	Mobile signature service checks the validity of requesting the mobile signature (e.g. correct MS-ISDN, signature expiry, etc.).
7	VALID mobile signature request… …the mobile signature request transferred to citizen's mobile device.
8	Mobile signature request received at citizen's mobile device.
9	Citizen reads content of the received mobile signature request and follows on-screen instructions to generate his/her mobile signature.
10	Citizen enters personal security information (e.g. a PIN-Code) to indicate understanding of the mobile signature request content and to confirm intention to proceed with the transaction.

USE CASE NAME - tba	
11	Mobile device returns mobile signature to mobile signature service.
12	Mobile signature service processes mobile signature received from citizen's mobile device.
13	Mobile signature service returns a POSITIVE *(i.e. mobile signature successful")* condition response to *[Application Name].* application.
14	Citizen receives confirmation at the mobile device that the mobile signature was processed correctly.
15	*[Application Name].*application uses mobile signature response to inform the transaction instruction decision and initiate associated actions *(e.g. the transaction instruction).*
16	Transaction completion receipt *(e.g. the transaction instruction)* notified to citizen's mobile signature webpage (Note: and perhaps also by email, etc.).
17	USE CASE ENDS.

Annex B:
User Experience of Use Case

Figures B.1 and B.2 are offered to provide an impression (only) of the end-user experience of mobile signature at the mobile device.

Implementations of the signing application may vary from smartcard issuer (i.e. mobile network operator) to smartcard issuer (i.e. mobile network operator). The most obvious variation being the language of the text displayed to the citizen (e.g. English, French, German...), etc.

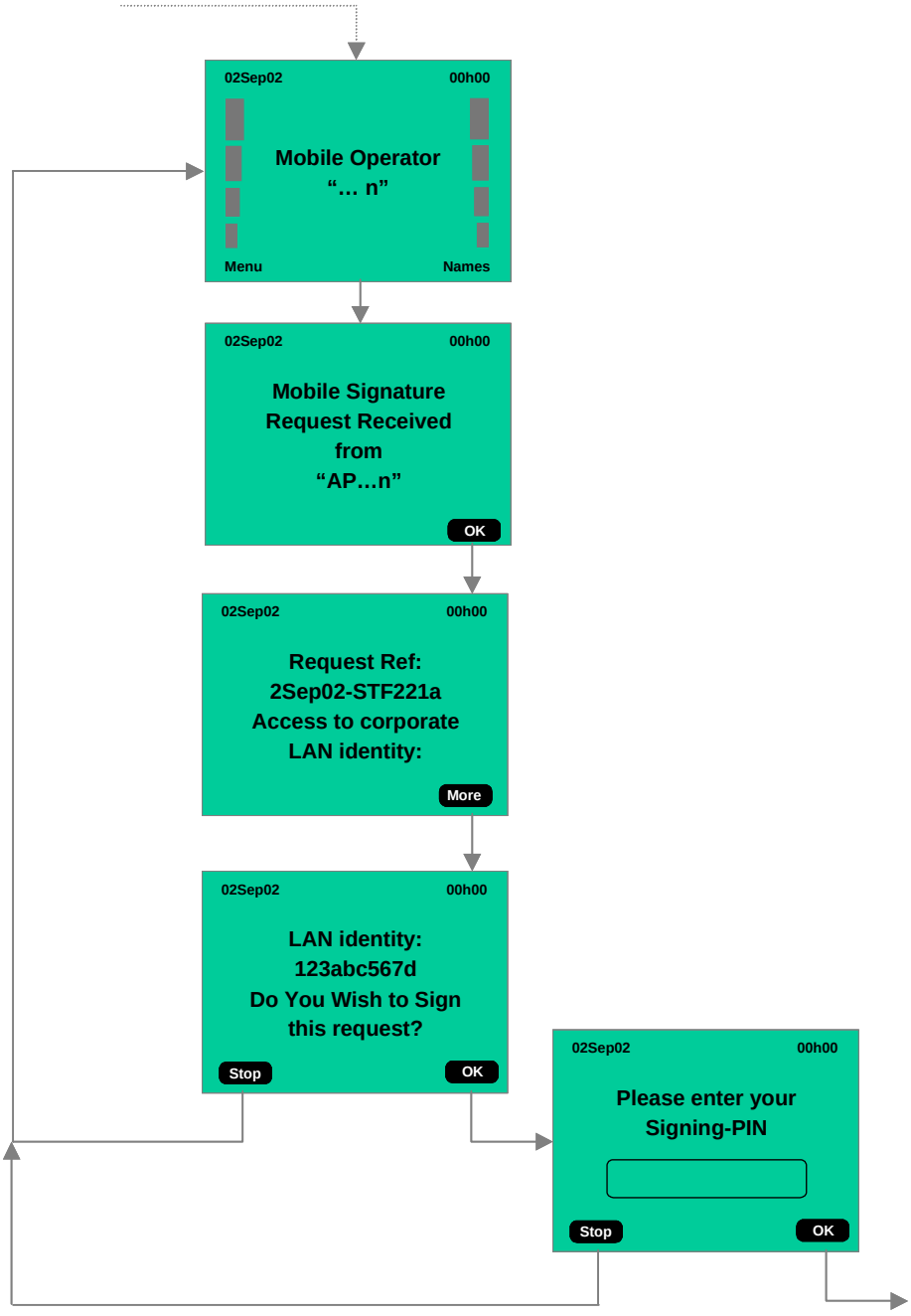


Figure B.1: End User Experience of Mobile Signature Use Case (Part 1)

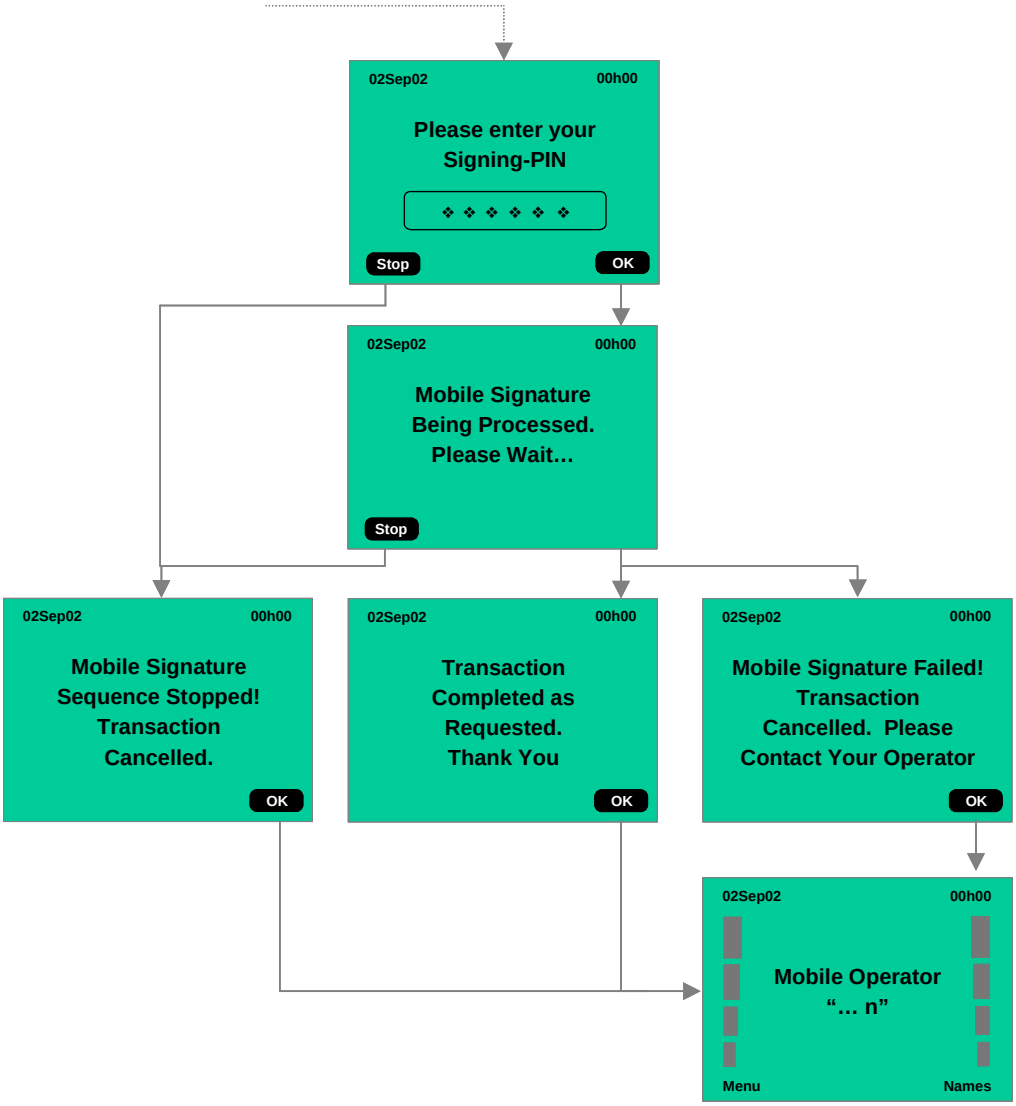


Figure B.2: End User Experience of Mobile Signature Use Case (Part 2)

Annex C: Bibliography

CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

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

CWA 14169: "Secure Signature-Creation Devices "EAL4+"".

CWA 14170: "Security Requirements for Signature Creation Applications".

CWA 14171: "Procedures for Electronic Signatures Verification".

CWA 14172-1: "EESSI conformance assessment guidance - Part 1: General".

CWA 14172-2: "EESSI conformance assessment guidance - Part 2: Certification Authority services and processes".

CWA 14172-3: "EESSI conformance assessment guidance - Part 3: Trustworthy systems managing certificates for electronic signatures".

CWA 14172-4: "EESSI conformance assessment guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification".

CWA 14172-5: "EESSI conformance assessment guidance - Part 5: Secure signature creation devices".

CWA 14355: "Guidelines for the implementation of Secure Signature-Creation Devices".

EESSI [http://www.ictsb.org/eessi/EESSI-homepage.htm] .

eEurope [http://eeurope-smartcards.org/], Global Interoperability Framework for Identification, Authentication and Electronic Signature (IAS) with Smartcards.

ICTSB [http://www.ict.etsi.fr/home.htm].

PKCS [http://www.rsasecurity.com/rsalabs/pkcs].

PKCS#1 (V1.2.1): "RSA Encryption Standard".

PKCS#7 (V1.5): "Cryptographic Message Syntax Standard".

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

IETF RFC 2396: "Uniform Resource Identifier (URI): Generic Syntax".

IETF RFC 2630: "Cryptographic Message Syntax".

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

ETSI TS 101 456 (V1.1.1): "Policy requirements for certification authorities issuing qualified certificates".

ETSI TS 101 733 (V1.3.1): "Electronic signature formats".

ETSI TS 101 862 (V1.2.1): "Qualified certificate profile".

ETSI TS 101 903 (V1.1.1): "XML Advanced Electronic Signatures (XAdES)".

ETSI TR 102 038 (V1.1.1): "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

ETSI TR 102 041: "Signature Policies Report".

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

ETSI TS 102 206: "Mobile Commerce (M-COMM); Mobile Signatures; Security Requirements for M-signatures Systems".

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

UMTS [http://www.umts-forum.org/].

WAP [http://www.wapforum.org/].

WLAN [http://standards.ieee.org/getieee802/802.11.html].

WSDL: "Web Services Description Language (WSDL) 1.1", W3C Note 15 March 2001.

XML-Schema 1: "XML Schema Part 1 : Structures".

XML-Schema 2: "XML Schema Part 2 : Datatypes".

IST-2001-38632: "T2R European Union Funded Project".

History

Document history		
V1.1.1	May 2003	Publication