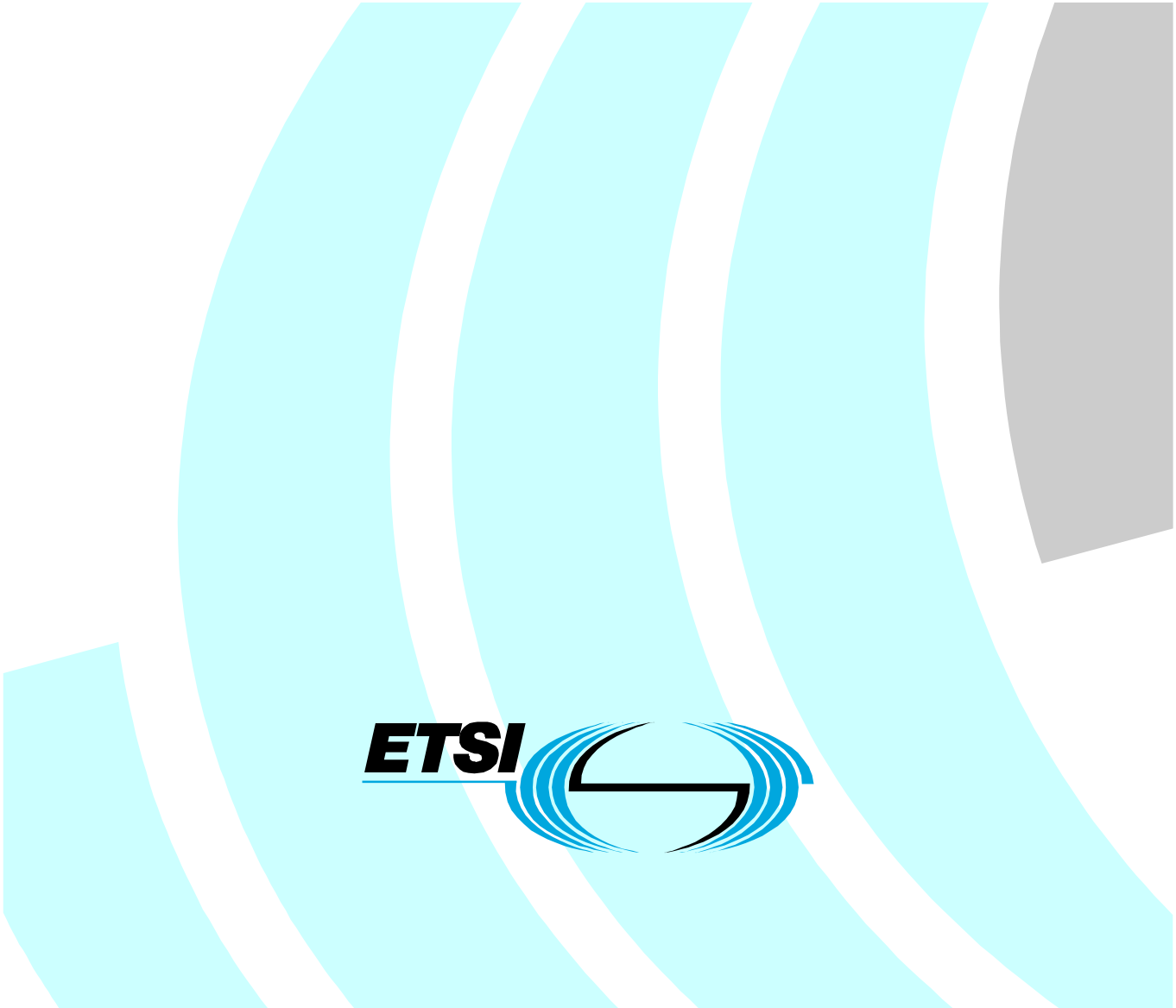
ETSI TS 102 207 V1.1.3 (2003-08)

Technical Specification

Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services



Reference
DTS/M-COMM-006

Keywords
commerce, electronic signature, M-commerce,
mobile, roaming, service

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Project M-Commerce (M-COMM).

Introduction

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

Consumers, businesses and government departments alike benefit in various ways. For the European Union (EU), electronic commerce presents an excellent opportunity to advance its programmes for economic integration. But, such an approach requires an appropriate security mechanism to allow completion of "remote" interactions between parties with confidence. To this end, the European Parliament and Council Directive on Electronic Signatures (1999/93/EC [2]) was published on December 13th, 1999.

The definition of "electronic signature" contained in article 2 of the Directive [2] 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 [2], the present document focuses on electronic signatures created by cryptographic means in a "secure signature creation device". As at June 2003, security provisions for signature creation and verification systems are such that parties wishing to provide a signature require "special" equipment. Typically, this involves a smartcard and a card reader with sufficient processing power and display capabilities to present full details of the transaction to be "signed". For consumer markets, however, it is doubtful whether individual citizens will want to invest in such equipment, which for the most part may remain connected to (or inserted into) personal computer equipment located in the home.

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

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

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

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

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

It is envisaged that mobile signature services will play a pivotal role in reaching an appropriate level of confidence, acceptance and interoperability to support implementation of the European Directive [2] on Electronic Signature - particularly for consumer (mass) markets. This Technical Report focuses on those technologies able to realize a mobile signature the equivalent of an "enhanced electronic signature" as defined by the European Directive [2].

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

- advising and guiding citizens about the use of mobile signature;
- acquiring mobile signature capability;
- managing citizen identity (including data protection and individual privacy);
- processing of signature requests from application providers (and providing responses);
- maintaining signature transaction records for the citizen;
- managing all aspects of signature lifecycle (e.g. validity, expiry);
- supporting service administration and maintenance activities.

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

- TR 102 203 [7]: "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements".
- TS 102 204 [8]: "Mobile Signature Service; Web Service Interface".
- TR 102 206 [9]: "Mobile Signature Service; Security Framework".
- TS 102 207 (the present document): "Mobile Signature Service; Specifications for Roaming in Mobile Signature Services".

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

1 Scope

Basically, an Application Provider should be able to get a Mobile Signature from any enduser, even if the Application Provider and the enduser have not contracted a commercial relationship with the same Mobile Signature Service Provider.

Otherwise, an Application Provider would have to build commercial terms with as many MSSPs as possible, and this might be a cost burden. This means that a Mobile Signature transaction issued by an Application Provider should be able to reach the appropriate Mobile Signature Service Provider, and this should be transparent for the Application Provider and the enduser. This is the concept of Mobile Signature Roaming.

The present document specifies technical interfaces over SOAP and HTTP for architectures that facilitate the roaming of mobile signature messages between the enduser and an Application Provider, and facilitate the building of an open model.

These standardized interfaces must allow:

- many-to-many relationships between stakeholders, relying parties and customers;
- both centralized or decentralized approach so that endusers and Application Providers are able to establish multiple trusted relationships;
- a minimized number of intermediaries between an enduser and an Application Provider;
- a common understanding between the Mobile Signature Service Provider and the Application Provider of the security involved in a mobile signature process;
- keep track of the path taken by the roaming transaction;
- a dispute resolution policy between Application Provider, Enduser, Home MSSP, Acquiring Entity and all the intermediaries involved in the roaming of the transaction.

1.1 Structure of this technical specification

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 [2].

Mobile Signature Roaming Service:

Specifies principles and requirements for the Mobile Signature Roaming Service. Also the Mesh concept is described.

Roaming Resolution:

This clause treats the negotiations that take place during a Mobile Signature Roaming transaction. The aim to find a path within the Mesh that targets the Mobile Signature Service Provider that is able to contact the enduser.

Scenarios:

This clause provides scenarios of how the Home Mobile Signature Service Provider of the enduser can be addressed by the Application Provider using the Mesh.

Technical Description of Roaming Service:

The technical description of the Roaming Service is outlined first and illustrated by means of message flows.

Data Formats:

The XML data types, i.e. SOAP Header blocks, used with respect to the Roaming Service are specified.

Processing Instructions:

Processing instructions with respect to the SOAP Header blocks are specified.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

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

[3] Liberty: "http://www.projectliberty.org".

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

[5] SOAP Version 1.2 Part 1: "Messaging Framework" and Part 2: "Adjuncts".

[6] Trusted Transaction Roaming T^2R: "Core Use Cases", Version 04, 14/02/03, http://www.radicchio.org/downloads/t2r_use_cases_14-02-03.pdf

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

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

[9] ETSI TR 102 206: "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework".

[10] W3C Recommendation 2 May 2001: "XML Schema Part 1: Structures" and "XML Schema Part 2 Datatypes".

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

EU Directive: directive 1999/93/EC [2] of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures

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

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

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

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

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

signature response: message sent from the Mobile Signature Service Provider to the Application Provider in response to a signature request

signer: person or entity that creates an electronic signature

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

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

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

specialist task force: ETSI temporary team of specialist assigned for specific purposes

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

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

web service: internet technology

3.2 Abbreviations

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

AE	Acquiring Entity
AMSSP	Acquiring MSSP
AP	Application Provider
API	Application Programming Interface
CA	Certification Authority
CC	Country Code
CEN	European Committee for Standardization
EESSI	European Electronic Signature Standardization Initiative
GSM	Global System for Mobile Communications
HMSSP	Home MSSP
IMSI	International Mobile Subscriber Identity
INMSI	International Mobile Station Identity
MNO	Mobile Network Operator
MS	Mobile Signature
MSISDN	Mobile Station Integrated Services Digital Network
MSS	Mobile Signature Service
MSSP	Mobile Signature Service Provider

PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
RA	Registration Authority
RE	Routing Entity
SN	Subscriber Number
STF-221	ETSI Specialist Task Force 221
TR	ETSI Technical Report
TS	ETSI Technical Specification
URI	Uniform Resource Identifier
VE	Verifying Entity
XML	eXtensible Markup Language

4 Void

5 Introduction to mobile signature

5.1 Overview

5.1.1 Mobile signature

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

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

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

Universal Method:

- a consistent end user experience;
- the largest interactive community for endusers and application providers;
- an architecture promoting interoperability and lowest deployment costs;
- an architecture offering the lowest transaction costs.

Mobile Device:

- any device using a mobile network as a communications channel;
- mobile telephone, PDAs, Laptop-PCs;
- 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 [2].

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.

5.1.2 Using mobile signature

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

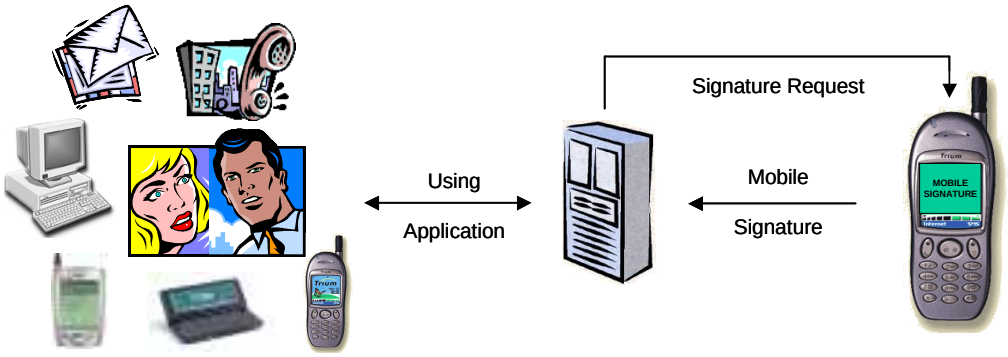


Figure 1: Mobile Device as "Signing Tool" (an electronic pen…)

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

5.1.3 Mobile signature service

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

- accelerate adoption of mobile signature by APs (and consequently adoption by endusers);
- allow implementation/deployment of a universal API;
- permit access to an existing base of endusers possessing smartcards and cardreaders;
- co-ordinate activation of mobile signature functionality for endusers;
- co-ordinate the processing of signature requests for application providers;
- add value to core mobile signature service (e.g. timestamp, receipt storage, signature verification, etc.);
- leverage existing customer support and communication mechanisms;
- resolve issues faced by "traditional" operators of CA platforms (user registration process, legalities, service level agreement);
- reduce service deployment costs;
- minimize duplication;
- aggregate (i.e. acquire) signature traffic;
- provide a manageable approach to risk reduction;

- promote interoperability.

A mobile signature service might be provided under the terms of a commercial agreement between a Mobile Signature Service Provider (MSSP) and those parties who choose to rely on mobile signatures for whatever reason. The features of the MSSP role and his/her responsibilities are considered in clause 13 of TR 102 203 [7].

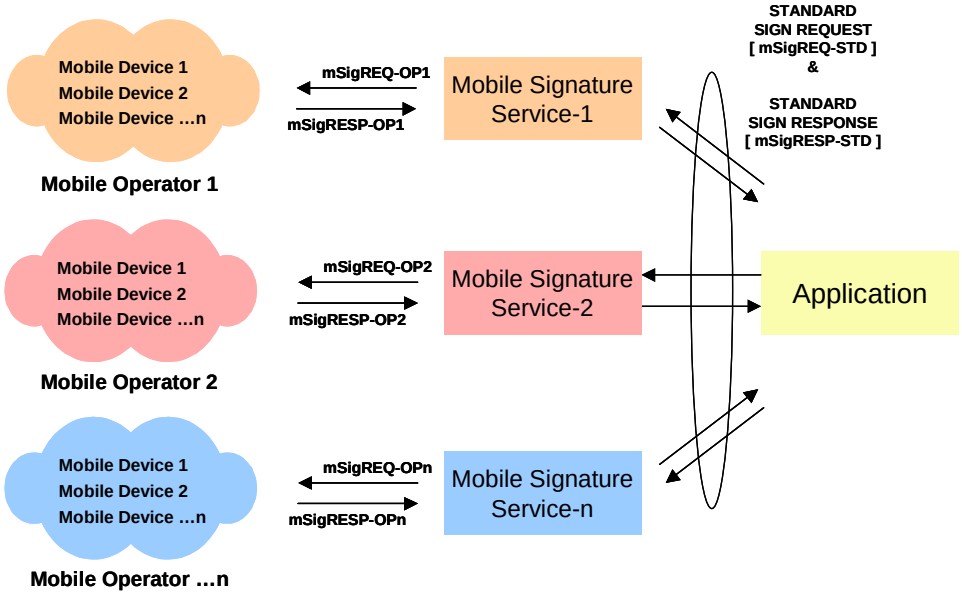


Figure 2: Mobile signature service

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

5.2 Notation

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

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in the present document are to be interpreted as described in RFC 2119 [4]. When these words are not capitalized, they are meant in their natural-language sense.

5.3 XML Schema declaration

The following XML namespace is used for the Roaming Service:

- http://uri.etsi.org/TS102207/v1.1.2#

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

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://uri.etsi.org/TS102207/v1.1.2#"
xmlns:env="http://www.w3.org/2003/05/soap-envelope"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msrs="http://uri.etsi.org/TS102207/v1.1.2#"
xmlns:mss=http://uri.etsi.org/TS102204/v1.1.2#
elementFormDefault="qualified"
>
```

This implies that the prefix mss is used throughout the present document to denote the namespace of the Mobile Signature Service according to TS 102 204 [8]. The prefix xs denotes the namespace of the XML-Schema specification [10] while the prefix env denotes the namespace of the SOAP envelope, see SOAP version 1.2 part 1 [5]. The prefix msrs is used to denote the namespace of the Roaming Service specified in the present document.

The provided XML-Schema is normative.

6 Mobile signature roaming service

This clause specifies principles and requirements for the Mobile Signature Roaming Service and describes the Mesh concept. This clause is based upon the work of the Trusted Transaction Roaming project, see [6].

6.1 Roaming issues

There are two major principles that a mobile Signature Service must follow TR 102 203 [7]:

- mobile signature service should promote and facilitate the largest addressable community of citizens (consumers) for the application provider community;
- mobile signature service should adopt an architecture promoting interoperability and lowest deployment costs.

According to what has been specified in TS 102 204 [8], the diagram below represents one of the situations an Application Provider may face.

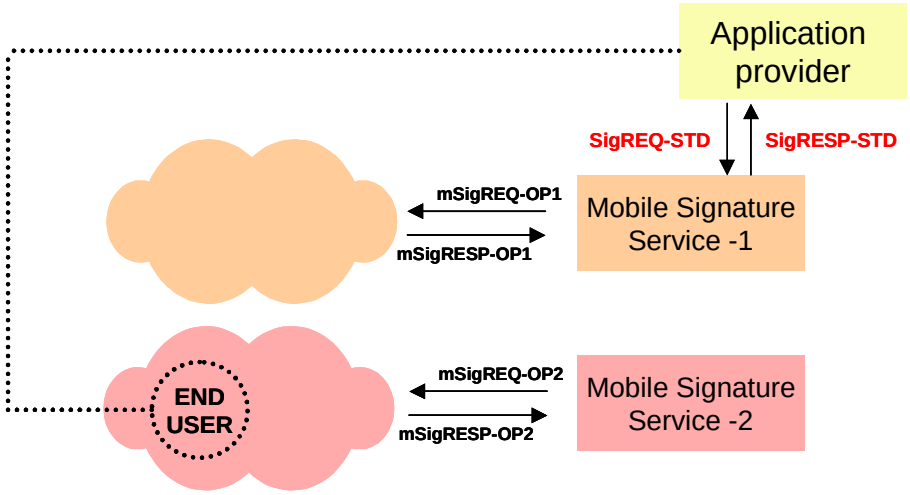


Figure 3: Mobile signature roaming issue

Basically, an AP should be able to get a Mobile Signature from any enduser, even if the AP and the enduser have not contracted a commercial relationship with the same MSSP. Otherwise, an AP would have to build commercial terms with as many MSSPs as possible, and this might be a cost burden. This means that a Mobile Signature transaction issued by an Application Provider should be able to reach the appropriate MSSP, and this should be transparent for the AP. This is the concept of Mobile Signature Roaming.

6.2 Interoperability domain: a mesh

Mobile Signature roaming itself requires commercial agreements between the entities that facilitate it. In this respect, we assume that various entities (including MSSPs) will join in order to define common commercial terms and rules corresponding to a Mobile Signature Roaming Service. This is the concept of a Mobile Signature Roaming Service, which the present document represents as a Mesh of members undertaking one or several of the following roles

NOTE: This list is not exhaustive:

- Acquiring Entity (AE): an entity performing this role is one of the entry points of the Mesh, and handles commercial agreements with APs. The entry point in the Mesh may be for instance a MSSP, or an aggregator of Application Providers in the context of a particular communities of interests (e.g. payment associations, banks, MNOs etc.). That's the reason why we define this more abstract role. An Acquiring Entity implements the Web Service Interface specified in TS 102 204 [8];
- Home MSSP (HMMSP): this is the MSSP that is able to deal with the current enduser and the current transaction;
- Routing Entity (RE): any entity that facilitates the communication between the AE and the home MSSP;
- Attribute Provider: this role is described by Liberty Alliance [3]. One or several mesh members may undertake this role and store relevant attributes in order to facilitate the discovery of the Home MSSP by other Mesh members;
- Identity Issuer: an entity that is able to make a link between a Mobile Signature and an enduser's identity. Within a PKI system, this is typically the CA and/or a RA;
- Verifying Entity (VE): an entity that can verify a Mobile Signature. A MSSP may be a Verifying Entity as well;
- Acquiring MSSP (AMSSP): this is a MSSP acting as an entry point in the Mesh. We can imagine that a commercial model for a mobile Signature Roaming Service is a Mesh of MSSPs which are fully or partially connected between each others.

Figure 4 shows the path taken by a mobile Signature transaction through the Mesh of a Mobile Signature Roaming Service. The mesh members encountered on the path may be any Identity Issuer, and/or any Verifying Entity and/or any Routing Entity.

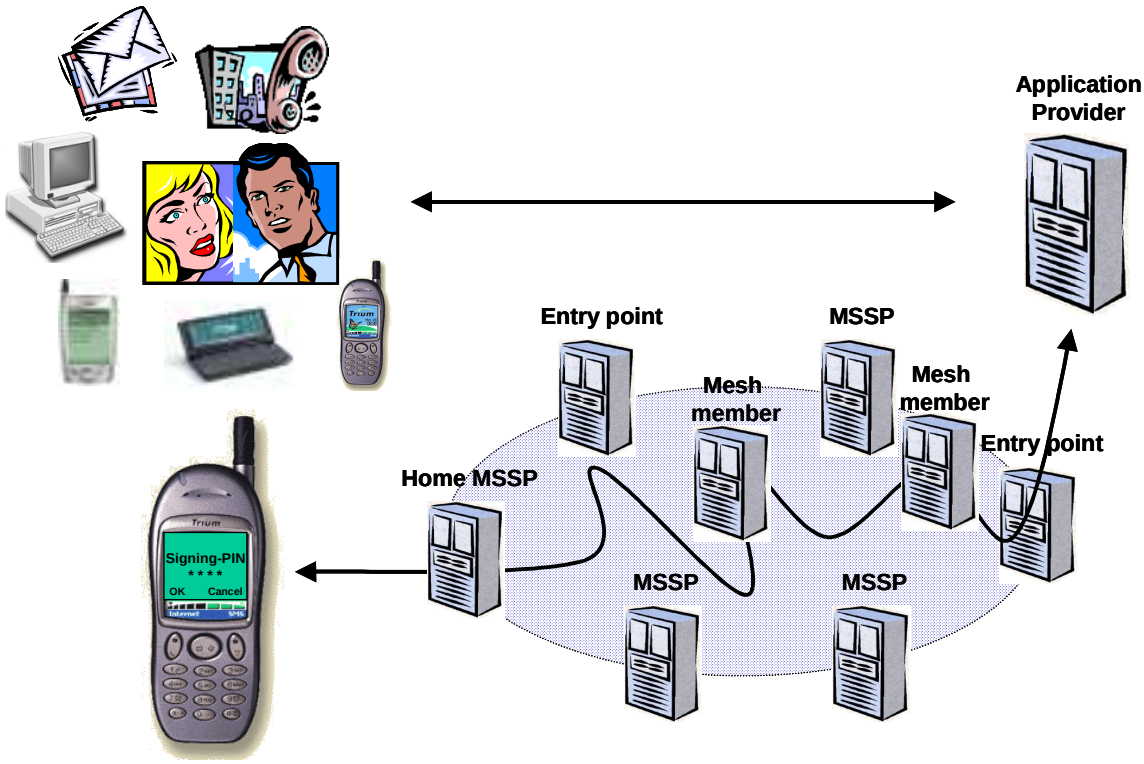


Figure 4: Mobile signature mesh

Within the mesh, different commercial ecosystems are possible. This technical specification doesn"t mandate any commercial ecosystem. To each ecosystem corresponds a technical implementation, with its own transaction flows. However, it is essential to identify as many models as possible in order to find out technical issues and propose some technical solutions.

6.3 Functional requirements

The present document specifies technical interfaces for architectures that facilitate the roaming of mobile signature messages between the enduser and an Application Provider, and facilitate the building of an open model.

That means that these standardized interfaces must allow:

- many-to-many relationships between stakeholders, relying parties and customers;
- both centralized or decentralized approach so that endusers and Application Providers are able to establish multiple trusted relationships;
- a minimized number of intermediaries between an enduser and an Application Provider;
- a common understanding between the home MSSP and the Application Provider of the security involved in a mobile signature process;
- keep track of the path taken by the roaming transaction;
- a dispute resolution policy between Application Provider, Enduser, Home MSSP, Acquiring Entity and all the intermediaries involved in the roaming of the transaction.

7 Roaming resolution

"Roaming resolution" represents the negotiations (inquiries, etc.) that occur during a mobile Signature Roaming in order to find a path within the Mesh which targets the right MSSP. Basically, this resolution depends on the commercial ecosystem that has been chosen within a Mesh. As we have said previously, it is outside the scope of this Technical Specification to work on the commercial ecosystems. However, the scenarios we have identified in clause 6 correspond to different commercial ecosystems. From the descriptions of these scenarios, we are able to identify potential technical requirements for different roaming resolution systems:

7.1 Discovery of the right home MSSP

This step must occur as soon as possible within the Mesh when a transaction occurs, e.g. by the Acquiring Entity. According to the information it might get (UserId, Identity Issuer, MSISDN), there are different possibilities for a Mesh member to discover the right MSSP:

MSISDN

In the case where a MSSP is hosted by a Mobile Network Operator (MNO), the right MSSP may be discovered from the enduser's mobile phone number thanks to the internal public telecommunication numbering plan E.164 of ITU which identifies and publishes number ranges and structure (All telephone numbers can be called if a number is dialled of up to 15 digits, made up of a one to three digits Country Code (CC), followed by the Subscriber Number (SN)). Updated databases of number ranges can be downloaded from the Web. Enduser's mobile phone number is the so called MSISDN (Mobile Station Integrated Services Digital Network).

It would be possible for any mesh member to get hold of the full database. Or else send infrequent queries to a web-site hosting the database. So, a Mesh member guesses the Home MSSP from number ranges and forwards to the guessed MSSP.

Owing to number portability, the user may have moved to another network. In that case the ported-from network returns the ported-to network as part of an error code, and the mesh member tries again with the correct Home MSSP. Alternatively, the ported-from Home MSSP itself forwards the MS Message to the ported-to Home MSSP. Up to June 2003, there is nothing that mandates this kind of rule from MNO.

However, in countries where porting is enforced by regulator, the requirement on the networks is not to deprive the user of any services that they would be entitled to if they had just changed subscription without porting the number. Therefore, a Mobile Signature Roaming Service should enforce this requirement and mandate it by mentioning it among the contractual agreements between the Mesh members.

IMSI

ITU-T Recommendation E.212 [1], defines a numbering plan for land mobile stations in international public land mobile networks (PLMN). It establishes the principles for allocation of International Mobile Station Identities (INMSI) to stations. For this purpose a so called IMSI has been defined. IMSI stands for International Mobile Subscriber Identity.

An IMSI is required so that a visited mobile network can identify a roaming mobile handset, terminal or user, in order to contact the subscriber's home network for subscription and billing information. This IMSI is used by all mobile operators in the world to be able to identify any mobile handset logged onto their network. An IMSI code therefore has worldwide validity.

The IMSI code is always made up of 15 digits and is unique in every network. The following information applies for mobile GSM networks. The IMSI codes consists of three parts, a three digits Mobile Country Code, a two digits mobile Network Code, and a ten digits mobile Station Identification Number.

Even if the MSISDN is portable, a new IMSI is supplied to the enduser during porting. So, one can be certain of reaching the right MNO by getting an enduser's IMSI. However, it is unlikely that an enduser knows his IMSI and provides it to an Application provider.

UserId and Identity Issuer

From the enrolment phase, the Identity Issuer is able to get and store the Home MSSP and the MSISDN of an enduser. Then, the Acquiring Entity is able to retrieve the enduser's MSISDN and Home MSSP address from the Identity Issuer. The Identity Issuer itself could be able to route the transaction to the right Home MSSP.

However, the Identity Issuer still has to discover the Home MSSP of the enduser at the enrolment phase. This can be performed thanks to the other described discovery systems (e.g. thanks to the MSISDN ranges, etc.).

If a Mesh Member queries an Identity Issuer in order to get information about the MSISDN and/or Home MSSP of the enduser or the Verifying Entity to be used, this interface is out of the scope of the Mobile Signature Service and therefore not considered in the present document. The reason is that other entities are working on a standardized interface to this kind of attribute providers, e.g. Liberty Alliance [3]. However, the Mobile Signature Service does cover the case that a Mesh Member makes use of an Identity Issuer as a Routing Entity i.e. the Mesh Member forwards a Mobile Signature transaction message to the Identity Issuer for onward routing.

Others…

In the case of centralized roaming systems, there may be different discovery systems. There are two different types of centralized roaming systems:

- centralized roaming systems that are based on the assumption that there is one particular Mesh member that stores a directory service where any Mesh member can get the Home MSSP address according to an enduser's identifier;
- centralized roaming systems where there is a central intermediary which is the only Acquiring Entity (that means the only entry point of the Mesh), and which is in charge of handling commercial agreements with MSSPs. In that case, The Acquiring Entity has likely a database making a link between an enduser's identifier and the right MSSP (the Home MSSP).

NOTE: An international decentralized roaming system can be based upon several centralized (e.g. national) roaming systems). In that case, we can say that a Mesh may be made of several sub-Meshes, for instance, one Mesh for each country of the European Community Mesh.

7.2 Finding a path through a mesh

Once any Mesh member has obtained the right MSSP address for this transaction and this enduser, the Mesh member has to contact the Home MSSP and route the Mobile Signature message. This is the step where we have to introduce the two concepts of "fully connected Mesh" and "partially connected Mesh".

Partially connected Mesh

All the Mesh members are not connected together (technically or commercially). That means that a Mesh member might need an additional Routing Entity in order to send a request to another Mesh member. In the case that one Routing Entity is not able to reach another RE it is up to the RE to decide whether or not to send the message once again or to try another path in the Mesh or to return an error message.

It is outside the scope of the Mobile Signature Service to specify how one Routing Entities knows which RE to contact in order to deliver a MS transaction message in the Mesh. These are one-off routing rules, which can be established whenever a new member joins the Mesh.

Fully connected Mesh

Any Mesh member can contact any Mesh member. In that case, there is no need for Routing Entities. Any Acquiring Entity is able to send directly a request to the Home MSSP of an enduser.

8 Scenarios

This clause provides scenarios of how the Home MSSP of the enduser can be addressed by the Application Provider using the Mesh. Based upon these scenarios and the general requirements for a Mobile Signature Roaming Service, the interfaces between the involved parties are identified and specified in the following clauses.

The presented scenarios deal with the case of a decentralized and of a centralized structure of the Mesh. Actually there is no central entity mentioned in the scenarios but all optional Routing Entities that can be in between the Acquiring Entity, the Identity Issuer, the Verifying Entity and the Home MSSP can be some kind of centralized entity.

Note that the Application Provider may be a part of the Mesh. In this case the AP fulfils also the role of the Acquiring Entity. So there is no need to exchange messages between the AP and the AE, but the AP can contact other members of the Mesh directly and vice versa.

In the case that there is (currently) no path to the Home MSSP in the Mesh (or back to the Acquiring Entity), an error message is returned to the Acquiring Entity (Home MSSP).

It is in principle not required that the path from the AE to the Home MSSP and the corresponding return path are the same. If a Verifying Entity is involved then the VE has to be part of both paths. Nevertheless for reasons of simplicity the Roaming service specified in the present document requires that both paths are the same.

8.1 Scenario 1

In this scenario the Acquiring Entity that is part of the Mesh has knowledge about the MSISDN and the Home MSSP of the enduser. E.g. these values are included in the Mobile Signature transaction message, i.e. the MSISDN and the Home MSSP and/or a user identifier and the corresponding Identity Issuer, see TR 102 204 [9]. Another possibility is that these values are known implicitly or can be retrieved by a service that is not subject to the Mobile Signature Service and therefore out of the scope of the present document.

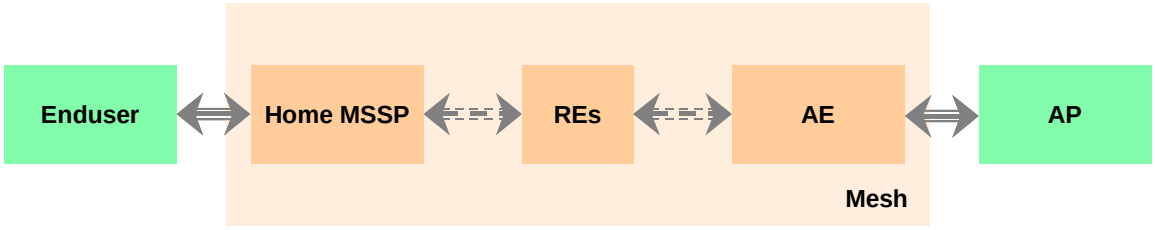


Figure 5: Scenario 1

- Precondition 1: The AE can retrieve the MSISDN and the Home MSSP of the enduser;
- Precondition 2: No Verification Service is required.

The following steps take place:

1. the AP provides a MS transaction message to an AE including the MSISDN, optionally the enduser's Home MSSP identifier, identifier of the enduser and the corresponding Identity Issuer (partial or complete);
2. the AE knows about the MSISDN and Home MSSP of the enduser (e.g. from the MS transaction message itself or from the enrolment phase) or can retrieve these values in a way that is out of the scope of the present document;
3. the AE sends the MS transaction message (possibly via Routing Entities, REs, of the Mesh) to the Home MSSP of the enduser;
4. this Home MSSP contacts the enduser;
5. the Home MSSP sends the response message of the MS transaction (this can also be an error message) to the AE (possibly via REs);
6. the AE sends the response message of the MS transaction to the AP.

8.2 Scenario 2

In this scenario the Acquiring Entity forwards the MS transaction message to the Identity Issuer of the user identifier specified in the MS transaction message. This Identity Issuer determines the Home MSSP (and the MSISDN) of the enduser and sends the MS transaction message to this Home MSSP possibly using other Routing Entities of the Mesh:

- Precondition 1: The AE has not sufficient knowledge about the MSISDN and Home MSSP of the enduser;
- Precondition 2: No Verification Service is required.

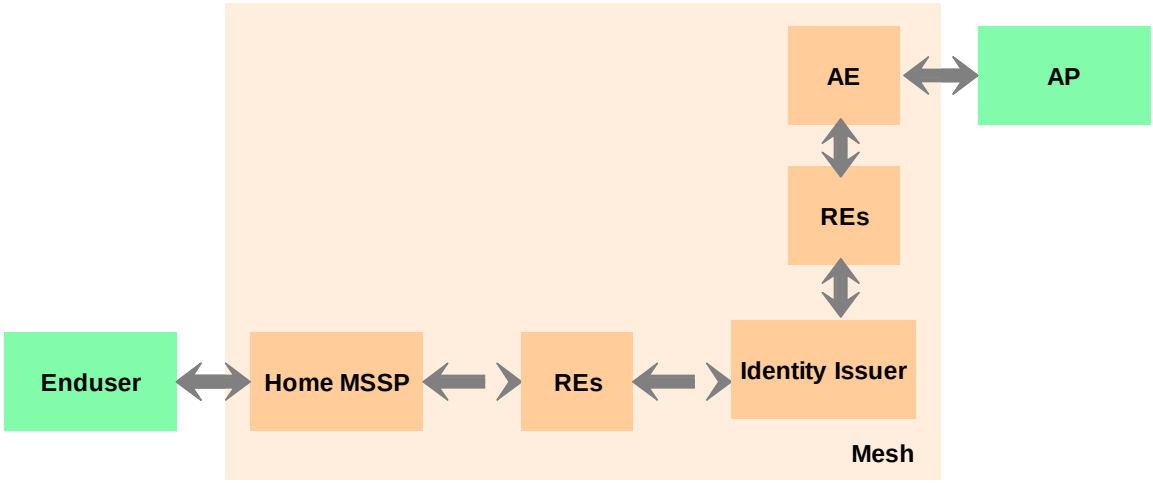


Figure 6: Scenario 2

The following steps take place:

1. the AP provides a MS transaction message to the AE including an identifier of the enduser and the corresponding Identity Issuer;
2. the AE forwards the MS transaction message to the Identity Issuer;
3. the Identity Issuer determines the MSISDN and Home MSSP of the enduser;
4. the Identity Issuer sends the MS transaction message (possibly via REs of the Mesh) to the Home MSSP of the enduser;
5. the Home MSSP contacts the enduser;
6. the Home MSSP sends the response message of the MS transaction (this can also be an error message) to the Identity Issuer (possibly via REs of the Mesh);
7. the Identity Issuer sends this response message to the AE;
8. the AE contacts the AP.

8.3 Scenario 3

In this scenario some kind of additional service (e.g. signature verification, timestamping, archiving) of a Verifying Entity is required in the MS transaction message. Therefore the transaction message is forwarded from the Acquiring Entity to the Verifying Entity that addresses then the Home MSSP:

- Precondition 1: A VE service is requested in the MS transaction message;
- Precondition 2: Either the AE or the VE is able to determine the MSISDN and the Home MSSP of the enduser. These values can be either known by the entities or retrieved from an Attribute Provider by an interface that is out of the scope of the Mobile Signature Service;

- Precondition 3: The AE is able to determine the VE to be used, e.g. the VE is denoted in the MS transaction message, implicitly known or retrieved by means of another service that is not specified in the context of the Mobile Signature Service.

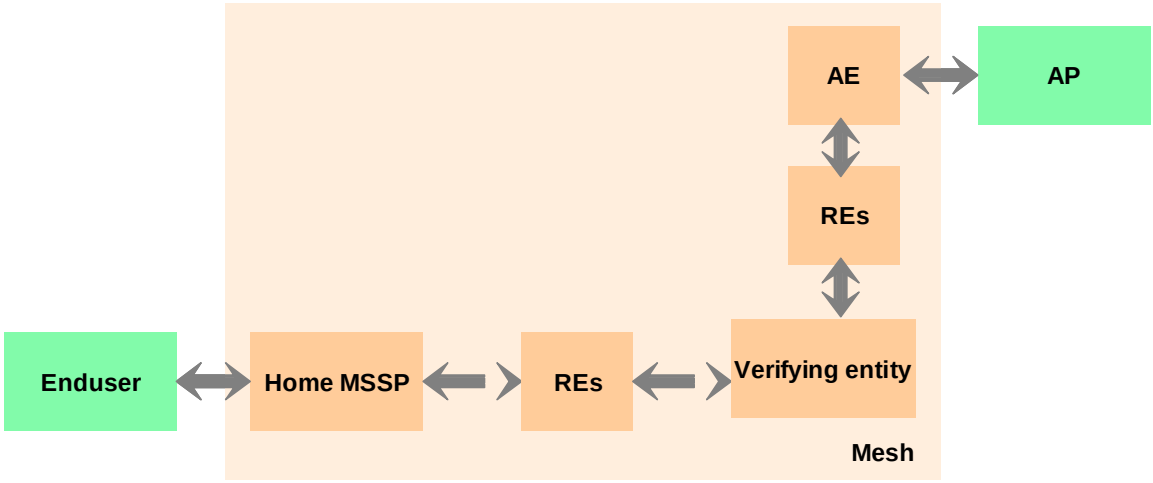


Figure 7: Scenario 3

In this scenario the following steps take place:

1. the AP provides a MS transaction message to the AE including the MSISDN, Home MSSP, user identifier of the enduser and the corresponding Identity Issuer (partial or complete);
2. if the AE knows about the MSISDN and Home MSSP of the enduser (e.g. from the MS transaction message itself or from the enrolment phase) this is included in the MS transaction message. The AE knows about or is able to determine the VE to be used;
3. the AE sends the MS transaction message (possibly via REs of the Mesh) to the VE;
4. the MSISDN and the Home MSSP is either specified in the MS transaction message, implicitly known by the VE or can be retrieved by means of a service that is not specified in the context of the Mobile Signature Service;
5. the VE sends the MS transaction message (possibly via REs of the Mesh) to the Home MSSP of the enduser;
6. the Home MSSP contacts the enduser;
7. the Home MSSP sends the response message of the MS transaction (this can also be an error message) to the VE (possibly via REs of the Mesh);
8. The VE applies the services requested by the AP and enduser and indicated in the MS transaction message that the VE received from the AE;
9. The VE sends this response message to the AE (possibly via REs of the Mesh);
10. The AE contacts the AP.

8.4 Scenario 4

In addition to scenario 3 the Verification Entity receives a MS transaction message from the AE without an indication of the Home MSSP and/or MSISDN. In order to send the MS transaction message to the corresponding Home MSSP the VE forwards the message to an Identity Issuer:

- Precondition 1: A VE service is requested in the MS transaction message;
- Precondition 2: The VE receives an MS transaction message from the AE without an indication of the Home MSSP and/or MSISDN;

- Precondition 3: The AE is able to determine the VE to be used, e.g. the VE is denoted in the MS transaction message, implicitly known or retrieved by means of another service that is not specified in the context of the Mobile Signature Service.

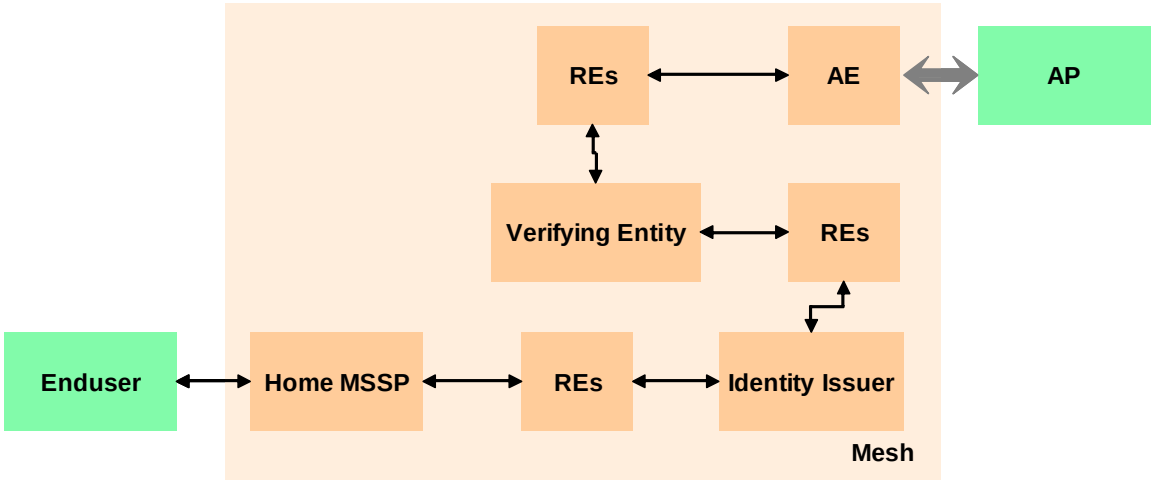


Figure 8: Scenario 4

In this scenario the following steps take place:

1. the AP provides a MS transaction message to the AE including the MSISDN, Home MSSP, user identifier of the enduser and the corresponding Identity Issuer (partial or complete);
2. the AE does not include any further information concerning MSISDN and/or Home MSSP in the MS transaction message. The AE knows about or is able to determine the VE to be used;
3. the AE sends the MS transaction message (possibly via REs of the Mesh) to the VE;
4. the VE forwards the MS transaction message to the Identity Issuer of the user identifier without any additional information concerning MSISDN and/or Home MSSP of the enduser;
5. the Identity Issuer determines the MSISDN and Home MSSP of the enduser;
6. the Identity Issuer sends the MS transaction message (possibly via REs of the Mesh) to the Home MSSP of the enduser;
7. the Home MSSP contacts the enduser;
8. The Home MSSP sends the response message of the MS transaction (this can also be an error message) to the Identity Issuer (possibly via REs of the Mesh);
9. the Identity Issuer sends this response message to the VE;
10. the VE applies the services requested by the AP and enduser and indicated in the MS transaction message that the VE received previously from the AE;
11. the VE sends the response message to the AE (possibly via REs of the Mesh);
12. the AE contacts the AP.

8.5 Scenario 5

In addition to scenario 4 the Acquiring Entity does not know which VE to use. Therefore the MS transaction message is forwarded to the Identity Issuer of the user identifier that can determine the corresponding VE by means that are not subject to the Mobile Signature Service specification (This implies that a user identifier and the corresponding Identity Issuer is specified in the MS transaction message):

- Precondition 1: A VE service is requested in the MS transaction message;
- Precondition 2: The AE is not able to determine the VE to be used, i.e. the VE is neither denoted in the MS transaction message nor implicitly known.

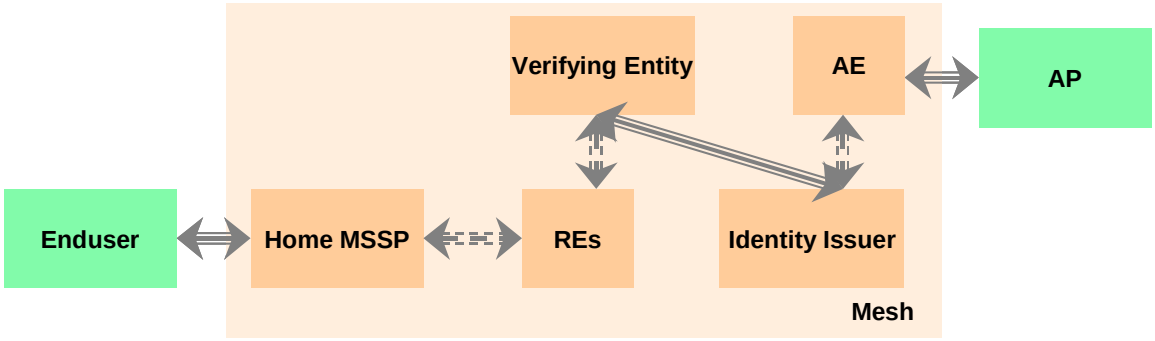


Figure 9: Scenario 5

In this scenario the following steps take place:

1. the AP provides a MS transaction message to the AE including the MSISDN and/or an identifier of the enduser and the corresponding Identity Issuer;
2. the AE does not know which VE to use. Therefore the MS transaction message is forwarded to the Identity Issuer specified in the MS transaction message;
3. the Identity Issuer determines the VE to be used by means that are not subject to the Mobile Signature Service specification. If the MSISDN and the Home MSSP are not specified in the MS transaction message the Identity Issuer determines this values as well. These values are added to the MS transaction message;
4. the Identity Issuer sends the MS transaction message (possibly via REs of the Mesh) to the VE;
5. the VE sends the MS transaction message (possibly via REs of the Mesh) to the Home MSSP of the enduser;
6. the Home MSSP contacts the enduser;
7. the Home MSSP sends the response message of the MS transaction (this can also be an error message) to the VE (possibly via REs of the Mesh);
8. the VE applies the services requested by the AP and enduser and indicated in the MS transaction message that the VE received previously from the Identity Issuer;
9. the VE sends this response message to the Identity Issuer (possibly via REs of the Mesh);
10. the Identity Issuer sends the response message to the AE (possibly via REs of the Mesh);
11. the AE contacts the AP.

9 Technical description of roaming service

In this clause the technical description of the Roaming service is outlined first and then illustrated by means of message flows. The technical details can be found in the following clauses.

9.1 Overview

The Mobile Signature Service is based upon the SOAP protocol, please refer to SOAP version 1.2 part 1 [5]. A SOAP message consists of a SOAP body and a SOAP header. The body contains in the case of the Mobile Signature Service a MSS request or response as specified in TS 102 204 [8]. The SOAP header contains in the case of the Mobile Signature Service an optional header block that contains a digital signature of the SOAP body.

SOAP provides means in order to use intermediary SOAP nodes in a message path using header blocks and the SOAP attributes "role", "mustUnderstand" and "relay". In the case of the Roaming service every Mesh Member acts as a SOAP node. These SOAP features are used in order to provide the Roaming service. Therefore additional headers and processing instructions with respect to these headers are specified in the present document. Different types of SOAP headers are used for the different entities; A RoutingHeaderType for every Mesh Member that routes a message, and additional header for Identity Issuers and Home MSSPs. These headers are specified in clause 10, the processing instructions are given in clause 11. The intermediary SOAP nodes used for the Roaming service only process SOAP header blocks not the SOAP body. I.e. the SOAP body itself is not altered on the way from the Mesh Entry Point to the Mesh End Point and vice versa.

9.2 Message flows

9.2.1 Mobile signature method using roaming

Figure 10 illustrates the usage of the Roaming service in conjunction with the Mobile Signature Service. As an example the Mobile Signature Method specified in TS 102 204 [8] is used. Please note that not all steps take place in the three different modes (synchronous, asynchronous client-server, asynchronous server-server) and that not all steps are part of the Roaming service. In this example the Acquiring Entity AE, the Routing Entities RE 1, RE 2 and the Home MSSP are Mesh Member. These entities can provide other services besides the Roaming service, e.g. a Routing Entity can be an Identity Issuer and provide information as the MSISDN or the Home MSSP.

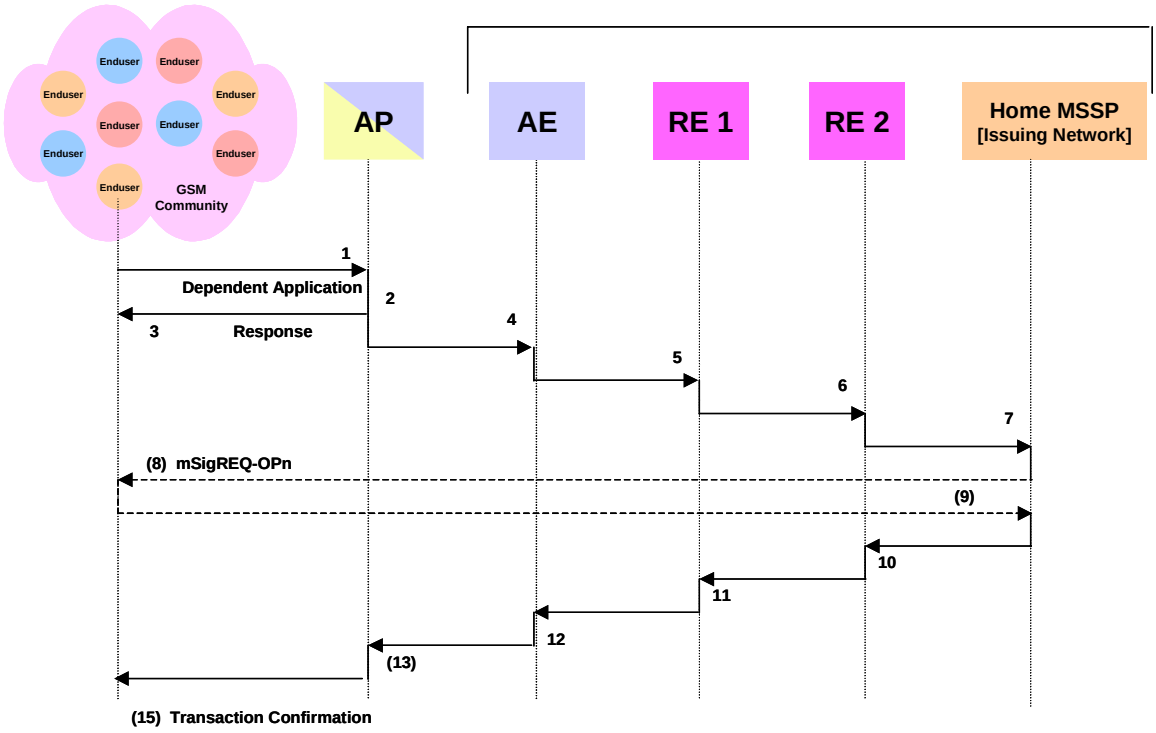


Figure 10: Mobile signature roaming flowchart

Steps 1 to 3 are neither part of the Roaming Protocol nor the Mobile Signature Service:

1: the Enduser confirms a transaction or wants to access a service;

2: the Application Provider AP processes enduser's confirmation and initiates data;

3: the 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.

Steps 4 is part of the Mobile Signature Service and makes no use of the Roaming service.

4: the Application Provider AP sends a SOAP message containing the MSS_SignatureReq to the Acquiring Entity AE.

The Acquiring Entity acts as a Mesh Entry Point and adds the SOAP header blocks required for the Roaming service to the SOAP message. This SOAP message is forwarded in the following steps to the Home MSSP. On the way to the Home MSSP additional information can be provided in the SOAP headers while the SOAP body is not altered, e.g. an Identity Issuer can provide the MSISDN and/or Home MSSP of the enduser using a SOAP header block.

Steps 5 to 7 are part of the Roaming Protocol as the Acquiring Entity is a Mesh Member, the so called Mesh Entry Point, as well as the Routing Entities RE 1 and RE 2 and the Home MSSP.

5: the Acquiring Entity sends the new SOAP message to the Routing Entity RE 1;

6: routing Entity RE 1 processes the relevant SOAP header block(s) according to the present document and sends the new SOAP message to Routing Entity RE 2;

7: routing Entity RE 2 processes the relevant SOAP header block(s) according to the present document and sends the new SOAP message to the Home MSSP.

The Home MSSP processes the relevant header blocks according to the present document and processes also the SOAP body, i.e. the MSS_SignatureReq.

In the case of the synchronous mode the Home MSSP contacts the enduser in steps 8 and 9 that are out of the scope of the Mobile Signature as well as the Roaming Service and answers then with a MSS_SignatureResp message. In the case of the asynchronous modes the Home MSSP answers first with a MSS_SignatureResp message and then contacts the enduser. This case is not displayed in the figure above.

In any case the Home MSSP generates a new SOAP message that contains in the SOAP body the MSS_SignatureResp message and an optional SOAP header block that contains an XML Signature using the SOAP body as input. In addition SOAP header with respect to the Roaming service are provided. The Home MSSP sends this SOAP message back to the Acquiring Entity by means of the Mesh using the same path as on the way from the Acquiring Entity to the Home MSSP.

10: the Home MSSP sends the new SOAP message to the Routing Entity RE 2;

11: routing Entity RE 2 processes the relevant SOAP header block(s) according to the present document and sends the new SOAP message to Routing Entity RE 1;

12: routing Entity RE 1 processes the relevant SOAP header block(s) according to the present document and sends the new SOAP message to the Acquiring Entity AE.

The Acquiring Entity acts as a Mesh End Point and processes the Roaming SOAP header according to the present document e.g. the Acquiring Entity deletes the SOAP header blocks that are relevant for the Roaming Service.

13: the Acquiring Entity sends the new SOAP message to the Application Provider AP.

9.2.2 Roaming error handling

In the case that an error occurs with respect to the Roaming service, the Mesh Member generates a SOAP fault that is included in the SOAP body and then returned. This SOAP fault is then forwarded to the Acquiring Entity that provides this error to the Application Provider.

The following diagram illustrates this behaviour. The same example as above is used, therefore steps 1 to 6 are the same.

7: routing Entity RE 2 processes the relevant SOAP header block(s) according to the present document and sends the new SOAP message to Routing Entity RE 3;

8: for any reason an error occurs. Routing Entity RE 3 generates a SOAP fault code and returns this fault code in the SOAP body. In addition it indicates that an error occurred.

In addition RE 3 creates a new set of header block(s) in order to return the message to the Acquiring Entity. RE 3 sends the new message to the Routing Entity RE 2.

9: routing Entity RE 2 processes the relevant SOAP header block(s) according to the present document. As specified in clause 7.2 (Partially connected Mesh) it is up to Routing Entity RE 2 to decide whether or not to send the message once again or to try another path in the Mesh or to return an error message. In this example RE 2 returns an error and sends the new SOAP message to Routing Entity RE 1;

10: routing Entity RE 1 processes the relevant SOAP header block(s) according to the present document and sends the new SOAP message to the Acquiring Entity AE.

The Acquiring Entity acts as a Mesh End Point and processes the Roaming SOAP header according to the present document e.g. the Acquiring Entity deletes the SOAP header blocks that are relevant for the Roaming Service.

11/12: the Acquiring Entity provides the SOAP fault to the Application Provider. Depending on the mode of the protocol either as a SOAP fault or as a MSS Status Response message, see TS 102 204 [8].

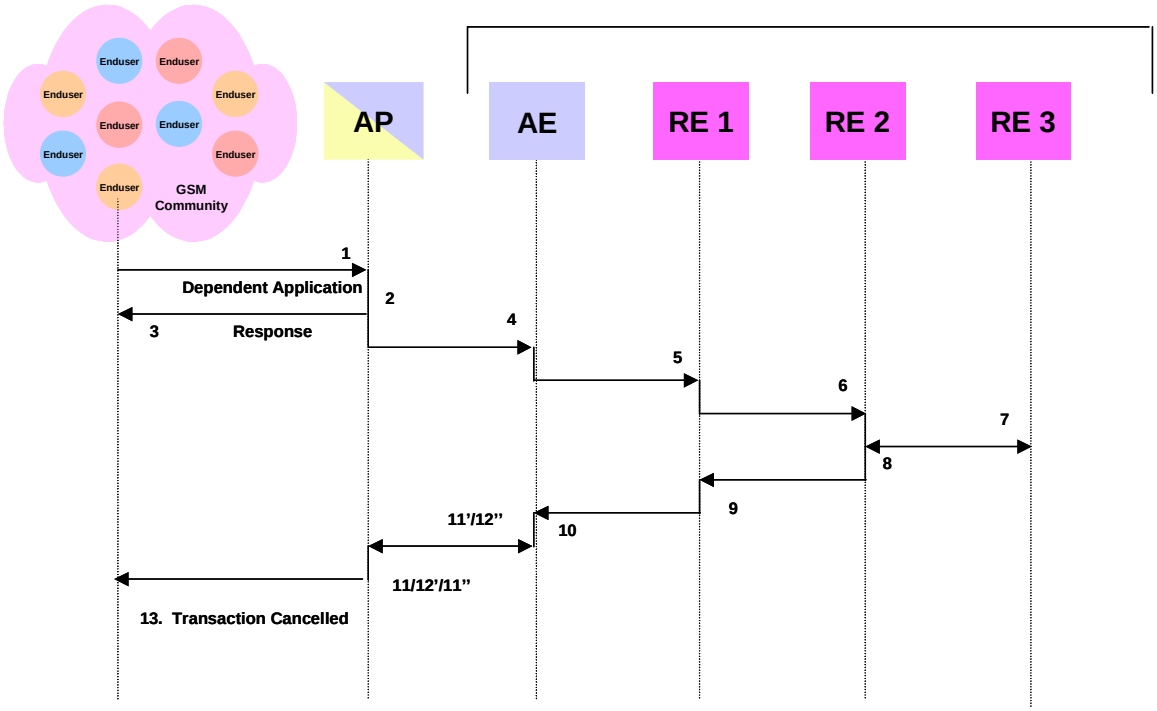


Figure 11: Error handling flowchart

10 Data formats

The XML namespace used in the present document and the prefixes used to denote other namespaces have already been defined in the introduction. In this clause the additional header blocks are described first and then the underlying XML-Schema types are presented. The processing instructions with respect to these header blocks are provided in the next clause.

10.1 SOAP header block types

10.1.1 Roaming header

A SOAP header block of the type RoamingHeaderType is processed by every Mesh Member that acts as a SOAP intermediary or as the SOAP ultimate receiver. The mandatory SOAP attribute role with the fixed value "next" indicates that this header MUST be processed by every intermediary including the ultimate receiver of the SOAP message chain. These nodes MUST process the header block according to the processing instructions presented in the next clause as indicated by the mandatory SOAP attribute "mustUnderstand". The value of this attribute MUST be set to "true". By means of the optional attribute "RoamingError" a SOAP node can indicate whether an error with respect to the Roaming service occurred or not. A SOAP node that receives a SOAP message where this flag is set to true, can decide whether or not to resend the message, to try another path in the Mesh or to return an error message to the previous node in the Mesh.

Every SOAP intermediary adds a further element of type RoamingHeaderEntryType while the element of type CommonHeaderType is common to all intermediary nodes. These types are presented below.

```
<xs:complexType name="RoamingHeaderType">
    <xs:sequence>
        <xs:element name="RoamingHeaderEntry" type="msrs:RoamingHeaderEntryType"
                                        maxOccurs="unbounded"/>
        <xs:element name="CommonHeader" type="msrs:CommonHeaderType"/>
    </xs:sequence>
    <xs:attribute ref="env:role" use="required" fixed="next"/>
    <xs:attribute ref="env:mustUnderstand" use="required"/>
<xs:attribute name="RoamingError" type="xs:boolean" use="optional"
                                                default="false"/>
    <xs>attribute name
</xs:complexType>
```

10.1.2 HMSSP header

A SOAP header block of the type HMSSP_HeaderType is processed by a Mesh Member that acts as Home MSSP with respect to the current Mobile Signature Service message. This Mesh Member MUST process the header block according to the processing instructions presented in the next clause as indicated by the mandatory SOAP attribute "mustUnderstand". The value of this attribute MUST be set to "true". The value of the mandatory SOAP attribute "role" MUST be set to the corresponding value specified for the Home MSSP role in clause 10.2.4. The optional attribute "HMSSP_Forward" is set by the Acquiring Entity and evaluated by the Home MSSP. If the user has moved to another network (owing to number portability), this flag determines whether the addressed Home MSSP shall forward the message to the new Home MSSP (in the case HMSSP_forward ="true" which is also the default value) or return a status message that includes the new Home MSSP (in the case HMSSP_Forward = false).

The type of the element HMSSP has been defined in the Mobile Signature Service XML schema. This element simply denotes the corresponding Home MSSP. In addition this type comprises the optional MSISDN of the enduser. An Identity Issuer can provide this information on the way from the Acquiring Entity to the Home MSSP. The any element provides means in order to extend the header block.

```
<xs:complexType name="HMSSP_HeaderType">
    <xs:sequence>
        <xs:element name="HMSSP" type="mss:MeshMemberType" minOccurs="0"/>
        <xs:element name="MSISDN" type="xs:string" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="HMSSP_Forward" type="xs:boolean" use="optional"
                                                  default="true"/>
    <xs:attribute ref="env:role" use="required"/>
    <xs:attribute ref="env:mustUnderstand" use="required"/>
</xs:complexType>
```

10.1.3 Identity issuer header

A Mesh Member that acts as an Identity Issuer with respect to the Mobile Signature Service transaction MUST process a header block of the type IdentityIssuer_HeaderType according to the processing instructions presented in the next clause. This is again indicated by the mandatory SOAP attribute "mustUnderstand". The value of the mandatory SOAP attribute "role" MUST be set to the corresponding value specified for the Identity Issuer role in clause 10.2.4.

The type of the element MobileUser has been defined in the Mobile Signature Service XML schema. This type denotes the Identity Issuer and comprises a user identifier. The Identity Issuer maps this identifier to a Home MSSP and/or an MSISDN. These values are provided by the Identity Issuer in the Home MSSP header block and the Identity Issuer header block is deleted after processing indicated by the absence of the SOAP "relay" attribute. The any element provides means in order to extend the header block.

```
<xs:complexType name="IdentityIssuer_HeaderType">
    <xs:sequence>
        <xs:element name="MobileUser" type="mss:MobileUserType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute ref="env:role" use="required"/>
    <xs:attribute ref="env:mustUnderstand" use="required"/>
</xs:complexType>
```

10.2 XML data types

10.2.1 Roaming header entry type

This data type consists of the following elements:

- the RE_SenderInfo element contains information about the Roaming Entity that is the sender of the Roaming message;
- the RE_Receiver element denotes the Roaming Entity (and its role) that is the receiver of the Roaming message;
- the attributes MajorVersion (currently 1) and MinorVersion (currently 1) denote the version of the MSS Roaming protocol (not of the MSS protocol itself).

```
<xs:complexType name="RoamingHeaderEntryType">
    <xs:sequence>
        <xs:element name="RE_SenderInfo" type="msrs:RE_SenderInfoType"/>
        <xs:element name="RE_Receiver" type="msrs:MeshIntermediaryNodeType"/>
    </xs:sequence>
    <xs:attribute name="MajorVersion" type="xs:integer" use="required"/>
    <xs:attribute name="MinorVersion" type="xs:integer" use="required"/>
</xs:complexType>
```

10.2.2 CommonHeader type

This data type contains all information common to the roaming process.

- the MeshStartPoint denotes either the Acquiring Entity (in the case that the message is sent from the AE to the HMSSP) or the HMSSP (in the case that the corresponding response message is sent from the HMSSP to the AE). Therefore the roles specified in clause 10.2.4 for the Acquiring Entity and the Home MSSP are used;
- the MeshEndPoint denotes either the HMSSP (in the case that the message is sent from the AE to the HMSSP) or the AE (in the case that the corresponding response message is sent from the HMSSP to the AE). This parameter is optional as the AE may not have sufficient knowledge about the HMSSP, but has to contact another entity for this reason. Therefore the roles specified in clause 10.2.4 for the Acquiring Entity and the Home MSSP are used;
- a MeshIntermediaryNode can be any Roaming Entity of the Mesh that has to be used on the path from the Mesh start point to the Mesh end point, e.g. an Identity Issuer or a Verifying Entity. This parameter is optional, more than one Mesh intermediary node can be specified. This element denotes a Mesh Member and the role of the Mesh Member, see clause 10.2.4;
- the MSS_Validity date contains the expiration date for the MSS transaction as specified in the message exchanged between the Application Provider and the Acquiring Entity;
- the AE_TransactionID is used to uniquely denote a chain in the Mesh for a roaming message starting at the AE;

- the HMSSP_TransactionID is used to uniquely denote a chain in the Mesh for a roaming message starting at the HMSSP.

```
<xs:complexType name="CommonHeaderType">
    <xs:sequence>
        <xs:element name="MeshStartPoint" type="msrs:MeshIntermediaryNodeType"/>
        <xs:element name="MeshEndPoint" type="msrs:MeshIntermediaryNodeType"
                                    minOccurs="0"/>
        <xs:element name="MeshIntermediaryNode"
                 type="msrs:MeshIntermediaryNodeType" minOccurs="0"
                                                 maxOccurs="unbounded"/>
        <xs:element name="CurrentMeshTarget"
                 type="msrs:MeshIntermediaryNodeType"/>
    </xs:sequence>
    <xs:attribute name="MSS_ValidityDate" type="xs:dateTime" use="optional"/>
    <xs:attribute name="AE_TransactionID" type="xs:NCName" use="required"/>
    <xs:attribute name="HMSSP_TransactionID" type="xs:NCName" use="optional"/>
</xs:complexType>
```

10.2.3 RE_SenderInfo type

This data type contains information about the Roaming Entity that has sent the Roaming message to the Receiver. The sender itself is specified by means of the MeshIntermediaryNodeType specified below. The sender specifies for every Roaming message a unique transaction ID and the time the message was created by the sender.

```
<xs:complexType name="RE_SenderInfoType">
    <xs:sequence>
        <xs:element name="RE_Sender" type="msrs:MeshIntermediaryNodeType"/>
    </xs:sequence>
    <xs:attribute name="RE_TransactionID" type="xs:NCName" use="required"/>
    <xs:attribute name="Instant" type="xs:dateTime" use="required"/>
    <xs:attribute name="TimeOut" type="xs:positiveInteger" use="optional"/>
</xs:complexType>
```

10.2.4 MeshIntermediaryNode type

This data type describes a Mesh Member by means of the MeshMemberType defined in the Mobile Signature Service XML schema. In addition information about the role of the Mesh Member is provided by means of the Mesh_Role attribute. The following values are specified for this purpose:

- http://uri.etsi.org/TS102207/v1.1.2#role_AcquiringEntity;
- http://uri.etsi.org/TS102207/v1.1.2#role_HomeMSSP;
- http://uri.etsi.org/TS102207/v1.1.2#role_IdentityIssuer;
- http://uri.etsi.org/TS102207/v1.1.2#role_RoutingEntity;
- http://uri.etsi.org/TS102207/v1.1.2#role_VerifyingEntity.

```
<xs:complexType name="MeshIntermediaryNodeType">
    <xs:sequence>
        <xs:element name="MeshMember" type="mss:MeshMemberType"/>
    </xs:sequence>
    <xs:attribute name="Mesh_Role" type="xs:anyURI" use="required"/>
</xs:complexType>
```

11 Processing instructions

In this clause the processing instructions with respect to the Roaming service are specified for every role of a Mesh Member. Please note that in addition to the interface specified in this protocol other interfaces can be used as well. E.g. an Acquiring Entity can contact an Identity Issuer by an interface other than the Roaming interface. In this case the processing instructions are of course obsolete - even if these instructions are denoted as mandatory using the expression "MUST".

11.1 Acquiring entity

An Acquiring Entity can act as a Mesh Entry and as a Mesh End Point. Therefore the processing instructions are presented in this clause for these two different roles.

If the Acquiring Entity has a direct connection to the Home MSSP, the Acquiring Entity can use the interface specified in TS 102 204 [8] directly.

11.1.1 Acquiring entity as mesh starting point

If the Acquiring Entity acts as a Mesh Start Point it MUST generate the SOAP header blocks required for the Roaming service, i.e. it MUST generate a Roaming Header and a HMSSP Header block. In the case that an Identity Issuer is used the Acquiring Entity MUST also create an Identity Issuer Header block.

The Acquiring Entity then forwards the new SOAP message (including the header blocks required for the roaming purposes) to the SOAP node indicated in the Roaming Entry element by means of the element RE_Receiver.

11.1.1.1 Roaming header block

Element / Attribute	Processing Instruction
RoamingHeaderEntry	The AE MUST provide this element according to the rules presented below.
CommonHeader	The AE MUST provide this element according to the rules presented below.
role	The value of this attribute MUST be set to "next".
mustUnderstand	The value of this attribute MUST be set to "true".
RoamingError	Absent or set to "false" (default value)

11.1.1.1.1 Common header

Element / Attribute	Processing Instruction
MeshStartPoint	This element denotes the AE itself. The AE MUST specify this value.
MeshEndPoint	If the corresponding Home MSSP is known from the Mobile Signature Service request the AE MUST specify this element.
MeshIntermediaryNode	The Mobile Signature Service messages MSS_SignatureReq, MSS_CertificationReq, MSS_RegistrationReq, MSS_ProfileReq, MSS_ReceiptReq contain an element MobileUser of the type MobileUserType. If this element specifies an Identity Issuer the AE MUST specify this entity by means of the MeshIntermediaryNode. The corresponding value of the attribute Mesh_Role MUST be set to the URI specified in clause 10.2.4. The Mobile Signature Service Message MSS_SignatureReq contains an optional element AdditionalServices in order to request additional services as signature validation, time stamping etc. If this element is specified the AE MUST specify these entities by means of the MeshIntermediaryNode. In addition a Routing Entity MAY add further MeshIntermediaryNodes that provide services which are out of the scope of the present specification. It is out of the scope of the present specification how the AE acquires knowledge about the order of the intermediary nodes.
MSS_ValidityDate	In the case of a MSS_SignatureReq and a MSS_CertificationReq the Mobile Signature Service Message can contain an optional attribute ValidityDate. If this attribute is present the AE MUST provide this value using this element.
AE_TransactionID	The AE MUST specify a unique (with respect to the AE) value. It is out of the scope of the present specification how to generate this value.
HMSSP_TransactionID	The AE MUST NOT specify a value for this element.
role	The value MUST be set to "next".
mustUnderstand	The value MUST be set to "true".

11.1.1.1.2 Roaming entry

Element / Attribute		Processing Instruction
RE_SenderInfo	RE_Sender	The value MUST be the same as the MeshStartPoint in the common header block.
	RE_TranactionID	The value MUST be the same as the AE_TransactionID in the common header block.
	Instant	The AE MUST provide the present time instant.
RE_Receiver		The AE MUST denote the SOAP receiver of the message. This is the first MeshIntermediaryNode specified in the Common Header. If no MeshIntermediaryNode is specified, it is the MeshEndPoint.
MajorVersion		The AE MUST set this value to the version used (the current major version is 1).
MinorVersion		The AE MUST set this value to the version used (the current minor version is 1).
MustUnderstand		The value of this attribute MUST be set to "true".

11.1.1.2 Home MSSP header block

The Acquiring Entity MUST create the Home MSSP header block according to the following rules.

Element / Attribute	Processing Instruction
HMSSP	Every Mobile Signature Service message contains an element MSSP_Info. If the MSSP_ID element is specified in the element MSSP_Info, the AE MUST copy this value to the element HMSSP of the Home MSSP header block.
MSISDN	The Mobile Signature Service messages MSS_SignatureReq, MSS_CertificationReq, MSS_RegistrationReq, MSS_ProfileReq, MSS_ReceiptReq contain an element MobileUser of the type MobileUserType. This element contains an optional element MSISDN. If this element is present in the Mobile Signature Service Message, the AE MUST copy the value to the element MSISDN of the Home MSSP header block.
HMSSP_Forward	The AE MAY specify this value. It is out of the scope of the present specification how the Acquiring Entity chooses this value.
role	The AE must specify the corresponding role of the Home MSSP, see clause 10.2.4.
MustUnderstand	The value of this attribute MUST be set to "true".

11.1.1.3 Identity issuer header block

If and only if an Identity Issuer is specified in the Mobile Signature Service request, the Acquiring Entity MUST create the Identity Issuer header block according to the following rules.

Element / Attribute	Processing Instruction
MobileUser	If the CommonHeader contains an element of type MeshIntermediaryNode that acts as an Identity Issuer, the AE MUST copy the element MobileUser from the Mobile Signature Service request message to the element MobileUser of the Identity Issuer Header block. If no Identity Issuer is used, the AE MUST NOT generate this header block.
role	The AE must specify the corresponding role of the Identity Issuer, cf. clause 10.2.4.
mustUnderstand	If this header block is present, the value of this attribute MUST be set to "true".

11.1.2 Acquiring entity as mesh end point

If the Acquiring Entity serves as a Mesh End Point the Acquiring Entity MUST remove all header blocks that are required for roaming purposes, i.e. all header blocks of the type:

- RoamingHeaderType;
- HMSSP_HeaderType;
- IdentityIssuer_HeaderType.

Then the Acquiring Entity sends the new SOAP message to the Application Provider.

11.1.2.1 Error handling

In the case that an error occurs with respect to the Roaming protocol the Acquiring Entity returns either a SOAP fault code or a MSS Status message, TS 102 204 [8].

11.2 Routing entity

Every Mesh Member acting as a SOAP intermediary acts as a Routing Entity with respect to the Mesh. A Routing Entity processes the Roaming Header block according to the rules presented below.

A Routing Entity can also act as an Identity Issuer, Home MSSP etc. Using the Roaming Header block the Routing Entity can determine whether it is supposed to act as Routing Entity or also as an Identity Issuer, Home MSSP etc. Therefore the element MeshIntermediaryNode provides also information about the Mesh role of the node. E.g. if the Mesh role Identity Issuer is indicated the node also processes the corresponding Identity Issuer Header.

The next intermediary SOAP node is given by the element MeshIntermediaryNode of the CommonHeader as this is an ordered list. If the Routing Entity is the last entry in this list, the next SOAP node is the MeshEndPoint. The Routing Entity MUST forward the new SOAP message to the next (intermediary) SOAP node.

11.2.1 Roaming header block

11.2.1.1 Common header

Element / Attribute	Processing Instruction
MeshStartPoint	The RE MUST not change this value.
MeshEndPoint	If the Home MSSP acts as MeshEndPoint the correct Home MSSP is not always known at the MeshEntryPoint. Therefore this value can be absent. If the RE acquires by any means knowledge about the Home MSSP the RE SHOULD provide this information using this element.
MeshIntermediaryNode	If the RE acquires by any means that are outside the scope of the present document knowledge about any further SOAP intermediaries the RE SHOULD add these nodes to this sequence. Please note that the order of the specified elements is of importance.
MSS_ValidityDate	The RE MUST not change this value. The RE MAY check the value. If the time period has expired the RE MAY respond with a SOAP fault code instead of forwarding the SOAP message.
AE_TransactionID	The RE MUST not change this value.
HMSSP_TransactionID	The RE MUST not change this value.
role	The RE MUST not change this value ("next").
mustUnderstand	The RE MUST not change this value ("true").

11.2.1.2 Roaming entry

Every Routing Entity adds a further Roaming Entry according to the following rules.

Element / Attribute		Processing Instruction
RE_SenderInfo	RE_Sender	This element denotes the RE itself. The RE MUST specify this value.
	RE_TranactionID	The RE MUST specify a unique (with respect to the RE) value. It is out of the scope of the present specification how to generate this value.
	Instant	The RE MUST provide the present time instant.
RE_Receiver		The RE MUST denote the SOAP receiver of the message.
MajorVersion		The RE MUST set this value to the version used (the current major version is 1).
MinorVersion		The RE MUST set this value to the version used (the current minor version is 1).
MustUnderstand		The value of this attribute MUST be set to "true".

11.2.2 Error handling

If the attribute RoamingError of the RoamingHeader is set to "true", the Routing Entity indicates that an error with respect to the Roaming service occurred. In this case, the Routing Entity throws a SOAP fault message. In the Roaming Header only a Roaming Header Entry is added.

The SOAP node that receives this error message can then decide to resent this message, to try another path or return an error message to the previous SOAP node. Depending on this decision the Roaming Header has to be changed.

11.3 Identity issuer

11.3.1 Roaming header block

The Identity Issuer handles the Roaming Header block as any other Routing Entity. By means of the Roaming Header the Identity Issuer determines that it is supposed to act as Identity Issuer and therefore processes the Identity Issuer Header block.

If the HMSSP is determined by the Identity Issuer, the Identity Issuer MUST set the HMSSP as MeshEndPoint in the Roaming Header block. It is out of the scope of the present specification what happens if another value is already specified as MeshEndPoint as the Identity Issuer itself is out of the scope of the present specification.

11.3.2 Identity issuer header block

The Identity Issuer makes use of the information provided in the Identity Issuer Header block in order to obtain the MSISDN and/or Home MSSP of the enduser. After processing the Identity Issuer Header block, the block is deleted. The Identity Issuer MUST provide the obtained values (MSISDN and/or Home MSSP) in the Home MSSP Header block.

11.3.3 Home MSSP header block

This header block is already present as the Acquiring Entity must create it.

Element / Attribute	Processing Instruction
HMSSP	If the HMSSP is determined by the Identity Issuer, the Identity Issuer MUST provide the HMSSP. It is out of the scope of the present specification what happens if another value is already specified.
MSISDN	If the MSISDN is determined by the Identity Issuer, the Identity Issuer MUST provide the MSISDN. It is out of the scope of the present specification what happens if another value is already specified.
HMSSP_Forward	The Identity Issuer does not change the value.
role	The Identity Issuer does not change the value.
mustUnderstand	The Identity Issuer does not change the value.

11.4 Home MSSP

Using the Roaming Header the Home MSSP determines that it is the Mesh End Point and supposed to act as Home MSSP. Therefore it processes the Home MSSP Header block.

The following cases have to be considered with respect to the Roaming service:

1: the Home MSSP is able to contact the enduser;

2: the enduser has changed the HMSSP owing to number portability, the value of the attribute HMSSP_Forward of the HMSSP header block equals "false";

3: the enduser has changed the HMSSP owing to number portability, the value of the attribute HMSSP_Forward of the HMSSP header block equals "true", the new Home MSSP is not a Mesh Member;

4: the enduser has changed the HMSSP owing to number portability, the value of the attribute HMSSP_Forward of the HMSSP header block equals "true", the new Home MSSP is a Mesh Member.

In the cases 1, 2 and 3 the Home MSSP returns a SOAP message to the Acquiring Entity, see TS 102 204 [8], by means of the Mesh. In case 4 the Home MSSP forwards the SOAP message to the new Home MSSP.

11.4.1 Roaming header block

11.4.1.1 Common header

In case 1, 2 and 3 a new Common Header is created according to the following rules.

Element / Attribute	Processing Instruction
MeshStartPoint	This element denotes the Home MSSP itself. The Home MSSP MUST specify this value.
MeshEndPoint	The Home MSSP MUST specify the Acquiring Entity AE as MeshEndPoint.
MeshIntermediaryNode	The HMSSP MUST specify the list of Mesh intermediaries that it received in reversed order.
MSS_ValidityDate	The HMSSP MUST NOT specify this element.
AE_TransactionID	The HMSSP MUST specify the value provided by the AE.
HMSSP_TransactionID	The HMSSP MUST specify a unique (with respect to the HMSSP) value. It is out of the scope of the present specification how to generate this value.
Role	The value MUST be set to "next".
mustUnderstand	The value MUST be set to "true".

In case 4 the received Common Header is changed according to the following rules.

Element / Attribute	Processing Instruction
MeshStartPoint	The HMSSP MUST NOT change this value.
MeshEndPoint	The HMSSP MUST change this value in order to denote the new HMSSP of the enduser.
MeshIntermediaryNode	The HMSSP MUST append itself as MeshIntermediaryNode regarding the order..
MSS_ValidityDate	The HMSSP MUST not change this value. The HMSSP MAY check the value. If the time period has expired the RE MAY respond with a SOAP fault code instead of forwarding the SOAP message.
AE_TransactionID	The RE MUST not change this value.
HMSSP_TransactionID	The RE MUST not change this value.
Role	The RE MUST not change this value ("next").
mustUnderstand	The RE MUST not change this value ("true").

11.4.1.2 Roaming entry

The Home MSSP adds an additional Roaming Entry as every other Routing Entity.

11.4.2 HMSSP header block

The information provided in the Home MSSP Header block (e.g. a MSISDN provided by an Identity Issuer) can be used in order to contact the enduser.

In case 1, 2 and 3 the Home MSSP Header block is deleted after processing.

In case 4 the HMSSP value is replaced and the new Home MSSP Header block is part of the new SOAP message that is sent (by means of the Mesh) to the new Home MSSP.

11.5 Verifying entity

By means of the Roaming Header the Verifying Entity determines that it is supposed to act as Verifying Entity. No SOAP header block is specified for a Verifying Entity as this entity must process the SOAP body for its services.

11.5.1 Roaming header block

The Verifying Entity handles the Roaming Header block as any other Routing Entity.

11.6 Error handling

The SOAP Fault mechanism is used in order to handle errors with respect to the Roaming service. The SOAP Fault mechanism is specified in clause 5.4 of SOAP 1.2 [5] Part 1 and has already been introduced in TS 102 204 [8]. The SOAP Fault element comprises the following elements:

- code;
- reason;
- node;
- role;
- detail.

The code element has a value, which can be among five SOAP standard codes, and contains application specific subcodes. These subcodes can contain further subcodes. Top level subcodes with respect to the SOAP fault code Sender and Receiver are specified in annex B for the Roaming service. Implementations MUST use this top-level subcodes and SHOULD indicate the fault code using subcodes of these top-level subcodes.

Annex B also provides reasons for the specified top-level subcodes. Implementations MUST use these reasons and SHOULD specify further reasontexts with respect to the implementation dependent subcodes.

Every SOAP node of the Mesh MUST specify a URI for the Node element.

Every SOAP node of the Mesh MUST specify its role using the URIs specified in clause 10 of the present document.

A SOAP node of the Mesh MAY provide further details with respect to its subcodes in the Detail element.

Annex A (normative): XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://uri.etsi.org/TS102207/v1.1.2#"
xmlns:env="http://www.w3.org/2003/05/soap-envelope"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msrs="http://uri.etsi.org/TS102207/v1.1.2#"
xmlns:mss="http://uri.etsi.org/TS102204/v1.1.2#"
elementFormDefault="qualified">
    <xs:import namespace="http://uri.etsi.org/TS102204/v1.00#"/>
    <xs:import namespace="http://www.w3.org/2003/05/soap-envelope"/>

    <xs:element name="HMSSP_Header" type="msrs:HMSSP_HeaderType"/>
    <xs:complexType name="HMSSP_HeaderType">
        <xs:sequence>
            <xs:element name="HMSSP" type="mss:MeshMemberType" minOccurs="0"/>
            <xs:element name="MSISDN" type="xs:string" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="HMSSP_Forward" type="xs:boolean" use="optional" default="true"/>
        <xs:attribute ref="env:role" use="required"/>
        <xs:attribute ref="env:mustUnderstand" use="required"/>
    </xs:complexType>
    <xs:element name="IdentityIssuer_Header" type="msrs:IdentityIssuer_HeaderType"/>
    <xs:complexType name="IdentityIssuer_HeaderType">
        <xs:sequence>
            <xs:element name="MobileUser" type="mss:MobileUserType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute ref="env:role" use="required"/>
        <xs:attribute ref="env:mustUnderstand" use="required"/>
    </xs:complexType>
    <xs:element name="RoamingHeader" type="msrs:RoamingHeaderType"/>
    <xs:complexType name="RoamingHeaderType">
        <xs:sequence>
            <xs:element name="RoamingHeaderEntry" type="msrs:RoamingHeaderEntryType"
maxOccurs="unbounded"/>
            <xs:element name="CommonHeader" type="msrs:CommonHeaderType"/>
        </xs:sequence>
        <xs:attribute ref="env:role" use="required" fixed="next"/>
        <xs:attribute ref="env:mustUnderstand" use="required"/>
        <xs:attribute name="RoamingError" type="xs:boolean" use="optional"
                                                    default="false"/>
    </xs:complexType>
    <xs:complexType name="RoamingHeaderEntryType">
        <xs:sequence>
            <xs:element name="RE_SenderInfo" type="msrs:RE_SenderInfoType"/>
            <xs:element name="RE_Receiver" type="msrs:MeshIntermediaryNodeType"/>
        </xs:sequence>
        <xs:attribute name="MajorVersion" type="xs:integer" use="required"/>
        <xs:attribute name="MinorVersion" type="xs:integer" use="required"/>
    </xs:complexType>
    <xs:complexType name="CommonHeaderType">
        <xs:sequence>
            <xs:element name="MeshStartPoint" type="msrs:MeshIntermediaryNodeType"/>
            <xs:element name="MeshEndPoint" type="msrs:MeshIntermediaryNodeType" minOccurs="0"/>
            <xs:element name="MeshIntermediaryNode" type="msrs:MeshIntermediaryNodeType"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="CurrentMeshTarget" type="msrs:MeshIntermediaryNodeType"/>
        </xs:sequence>
        <xs:attribute name="MSS_ValidityDate" type="xs:dateTime" use="optional"/>
        <xs:attribute name="AE_TransactionID" type="xs:NCName" use="required"/>
        <xs:attribute name="HMSSP_TransactionID" type="xs:NCName" use="optional"/>
    </xs:complexType>
    <xs:complexType name="RE_SenderInfoType">
        <xs:sequence>
            <xs:element name="RE_Sender" type="msrs:MeshIntermediaryNodeType"/>
        </xs:sequence>
        <xs:attribute name="RE_TransactionID" type="xs:NCName" use="required"/>
        <xs:attribute name="Instant" type="xs:dateTime" use="required"/>
        <xs:attribute name="TimeOut" type="xs:positiveInteger" use="optional"/>
    </xs:complexType>
    <xs:complexType name="MeshIntermediaryNodeType">
```

```
        <xs:sequence>
            <xs:element name="MeshMember" type="mss:MeshMemberType"/>
        </xs:sequence>
        <xs:attribute name="Mesh_Role" type="xs:anyURI" use="required"/>
    </xs:complexType>
</xs:schema>
```

Annex B (normative): SOAP fault subcodes

The following top-level subcodes are specified associated to the SOAP fault code Sender:

Subcode	Reason	Meaning
701	A Roaming Header block is missing.	A SOAP node that acts as Routing Entity makes use of this subcode if the Roaming Header block is absent.
702	An Identity Issuer Header block is missing.	A SOAP node that acts as an Identity Issuer makes use of this subcode if the Identity Issuer Header block is absent.
703	A Home MSSP Header block is missing.	A SOAP node that acts as an Identity Issuer makes use of this subcode if the Home MSSP Header block is absent. A SOAP node that acts as a Home MSSP makes use of this subcode if the Home MSSP Header block is absent.
710	Appropriate input information is missing.	A SOAP node makes use of this subcode if appropriate information is missing in the header blocks.
720	The validity date of the transaction has expired	If a SOAP node processes the MSS_ValidityDate element of the Roaming Header and this date has expired the SOAP node makes use of this subcode.

The following top-level subcodes are specified associated to the SOAP fault code Receiver:

Subcode	Reason	Meaning
750	Unable to provide Routing Entity services.	A Mesh Member makes use of this subcode if it can not forward the message for any reason.
760	Unable to provide Identity Issuer services.	An Identity Issuer makes use of this subcode if it can not provide Identity Issuer services for any reason (e.g. the specified user ID is unknown).
770	Unable to provide Verifying Entity services.	A Verifying Entity makes use of this subcode if it can not provide Verifying Entity services for any reason.
780	Unable to provide services.	An entity that does not act as a Routing Entity, Identity Issuer, Home MSSP or Verifying Entity makes use of the subcode if it can not provide its services for any reason.

Annex C (informative): Bibliography

- EESSI http://www.ictsb.org/eessi/EESSI-homepage.htm.
- IETF RFC 2396: "Uniform Resource Identifier (URI): Generic Syntax".

History

Document history		
V1.1.3	August 2003	Publication