Mobile Certificate based Healthcare Services

Farzan Yazdani

Degree Thesis

Information and Media Technology

2012

DEGREE THESIS	
Arcada	
Degree Program:	Information and Media Technology
Identification number:	3725
Author:	Farzan Yazdani
Title:	Mobile Certificate based Healthcare Services
Supervisor (Arcada):	Dr.Tech Göran Pulkkis
Commissioned by:	Arcada

Abstract:

This thesis work is a study of how the Mobile Signature Service (MSS) standard can be used in IT services of health centres. The study includes proposals of various mobile certificate based services that are appropriate for health centres and how these services can be realized. It is also described what is required from health centre users and health centre personnel to use the IT services.

The theoretical part describes how mobile certificates are deployed in Finland and how the Application Provider's Interface (API) is used. How the mobile signature service (MSS) is created, managed and processed is described from the API's point of view.

In the practical part various mobile certificate based solutions for health centres are proposed. The mobile certificate uses the MSS as the service for a transaction, which the user has initiated. The MSS in this thesis is based on authentication, signature of plain text content, and signature of digest content. Several tested solutions of the proposed mobile certificate based services are described.

Keywords:	Mobile Certificate, Mobile Certificate based Services, Mobile Signature Service, Mobile signature, FiCom, Healthcare, ETSI, Laverca
Number of pages:	50
Language:	English
Date of acceptance:	30.4.2012

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	3725
Författare:	Farzan Yazdani
Arbetets namn:	Digitala hälsovårdstjänster baserade på mobilcertifikat
Handledare (Arcada):	Dr.Tech Göran Pulkkis
Uppdragsgivare:	Arcada

Sammandrag:

Examensarbetet är en utredning om hur standarden Mobile Signature Service (MSS) kan utnyttjas i hälsostationer vid autentisering och digital signering i IT-tjänster. I arbetet utarbetas förslag till olika MSS-baserade tjänster som är lämpliga för hälsostationer samt hur dessa tjänster kan förverkligas. I arbetet beskrivs vad det krävs av hälsostationens användare och personal vid användning av IT-tjänsterna.

Den teoretiska delen beskriver hur mobilcertifikat används i Finland och hur tjänsteleverantörens gränssnitt (API) används. Hur mobil signaturtjänsten (MSS) skapas, hanteras och bearbetas beskrivs från tjänsteleverantörens synvinkel.

Den praktiska delen föreslås olika mobilcertifikatbaserade lösningar för hälsostationer. Mobilcertifikatet använder MSS som tjänst för en transaktion, som användaren har inlett. I detta examensarbete baseras MSS på autentisering, signering av ett textinnehåll och signering av ett s.k. fingeravtryck av en fil. Flera lösningar baserade av de föreslagna mobilcertifikattjänsterna är testade och beskrivna i examensarbetet.

Nyckelord:	Mobilcertifikat, Mobilcertifikatbaserade tjänster, Mobil signaturtjänst, Mobil signatur, FiCom, Hälso- och sjukvård, ETSI, Laverca
Sidantal:	50
Språk:	Engelska
Datum för godkännande:	30.4.2012

OPINNÄYTE	
Arcada	
Koulutusohjelma:	Tieto- ja mediatekniikka
Tunnistenumero:	3725
Tekijä:	Farzan Yazdani
Työn nimi:	Mobiilivarmennepohjaiset terveyspalvelut
Työn ohjaaja (Arcada):	Dr.Tech Göran Pulkkis
Toimeksiantaja:	Arcada

Tiivistelmä:

Opinnäytetyö on tutkimus siitä, miten Mobile Signature Service (MSS)-standardia voidaan käyttää terveyskeskuksien tietotekniikkapalveluissa. Tutkimus sisältää ehdotuksia eri mobiilivarmenteeseen perustuvista palveluista, jotka soveltuvat terveyskeskuksiin sekä miten nämä palvelut voidaan toteuttaa. Lisäksi kuvataan, mitä vaaditaan terveyskeskuksen käyttäjiltä ja terveyskeskuksen henkilökunnalta ehdotettujen tietotekniikkapalvelujen käytössä.

Teoriaosuudessa kuvataan mobiilivarmenteiden käyttöä Suomessa ja miten sovellustoimittajan rajapintaa (API) käytetään. Miten mobiilivarmenne allekirjoitus (MSS) luodaan, hallinnoidaan ja verifioidaan kuvataan API-näkökulmasta.

Käytännön osuudessa ehdotetaan mobiilivarmenneratkaisuja terveyskeskuksille. Mobiilivarmenne käyttää MSS palveluna käyttäjän aloittamassa transaktiossa. Tässä opinnäytetyössä perustuu MSS identiteetin todentamiseen, tekstisisällön allekirjoitukseen ja tiedostotiivisteen allekirjoitukseen. Useiden ehdodettujen mobiilivarmennepalvelujen testaus kuvataan.

Avainsanat:	Mobiilivarmenne, Mobiilivarmennepalvelua, Matkapuhelinallekirjoituspalvelu, Matkapuhelinallekirjoitus, FiCom, Terveyspalvelut, ETSI, Laverca
Sivumäärä:	50
Kieli:	Englanti
Hyväksymispäivämäärä:	30.4.2012

CONTENTS

Figures

Abbreviations & definitions

AE	Acquire Entity, the AE offers a Web Service Interface to an AP for a mobile signature service complying with the FiCom recommendation.
AP	Application Provider, the AP needs the User's signature and is AE's customer.
AP_ID	Application Provider's contact information in MSSP systems
AP_PWD	Application Provider's password in AE's system
CA	Certificate Authorities
ETSI	European Telecommunications Standards Institute
FiCom	Finnish Federation for Communications and Teleinformatics
FTP	File Transport Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HMSSP	Home Mobile Signature Service Provider, the user's home operator
ICT	Information and communications Technology
IIS	Internet Information Service
ISO	International Organization for Standardization
IVR	Interactive Voice Response
JSP	Java Server Page
MAC	Message Authentication Code
MSISDN	Mobile Subscriber Integrated Services Digital Network Number

MSS	Mobile Signature Service
MSSP	Mobile Signature Service Provider, MSSP provides HMSSP services to Users and potentially AE services to AP and/or AEs.
MSSPAPI	Mobile Signature Service Provider Application Programming Interface
NTP	Network Time Protocol
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKCS	Public-key cryptography
RE	Routing Entity, RE routes traffic between an AE and an HMSSP. RE can be component of AE or HMSSP systems or separate system of a TTP.
SAML	Security Assertion Markup Language
SIM	Subscriber Identity Module
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TTP	Trusted Third Party
UCS2	Universal Character Set – 2-bit
UICC	Universal Integrated Circuit Card
USSID	Unstructured Supplementary Service Data
UTF-8	Universal Character Set (UCS) Transformation Format – 8-bit
VPN	Virtual Private Network
WSDL	Web Services Description Language
XML	Extensible Markup Language

ACKNOWLEDGEMENTS

I would like to express my gratitude towards this opportunity to my supervisor and lecturer, Göran Pulkkis, who has been giving me the supports, ideas and advices during my Thesis writing process. I would also like to express my appreciation to the lecturers in Arcada, Magnus Westerlund, Jonny Karlsson, Johnny Biström and Hanne Karlsson for the knowledge and experience that they have shared during my educational time in Arcada.

I would like to dedicate this Thesis work to my parents and brother, who have given me the love and support both financially and intellectually.

Last but not least, I would like to say thank you to my dear friend Sebastian Lönnfors, who has been very kind and supportive by sharing the knowledge and helping me during my Thesis work.

Helsinki in April 2012
Farzan Yazdani

1 INTRODUCTION

Electronic services are growing rapidly and the lack of security, compatibility and effectiveness is one of the reasons why new methods like mobile certificate will play a big role in the evolution.

The mobile certificate is based on the ETSI's Mobile Signature Service (MSS) standards and has been developed in Finland in collaboration with mobile operators (Mobiilivarmenne, 2010). The MSS is used to give permission to a transaction (e.g. financial), which the user has initiated with his/her mobile device (ETSI, 2003b:13). Therefore the MSS is defined as a service were the mobile signature process is coordinated or managed for the user and for the application provider (AP) (ETSI, 2003a:7). The Mobile Signature Service Provider (MSSP) offers MSS systems for service providers (ETSI, 2003b:14).

In Web Service Interfaces the MSS is used for authentication or for signing text content or a digest of a content. Therefore MSS has a Web Service Interface, which MSSP provides and/or implements for an AP. (ETSI, 2003b:13)

1.1 Background

This thesis is written for health administration of Espoo. Espoo, the second largest city in Finland, provides a range of services for its residents, companies, employees, and visitors. The services include city administration, culture, education, social and health services etc. One of the important services is the social and health service, which offers the residents versatile wellness services.

The services of social and health centres in Espoo are constantly being developed. Espoo has created collaborative projects with universities, including Arcada University of Applied Sciences, to improve Espoo's social and health services. This thesis is a contribution to the collaborative project with Arcada.

1.2 The goal of thesis

The thesis is divided into a theoretical and a practical part. The theoretical part is a literature survey of the topic. The practical part is a collection of proposed mobile certificate based solutions for health centre IT services. Tests results of some proposed solutions are also presented.

To develop various mobile certificate based solution proposals, there is a need of understanding the concept of MSS. Therefore the theoretical part describes the needed knowledge of how the MSS is managed and processed to develop solutions for mobile certificate based services described in this thesis.

In the practical part, the development of various mobile certificate based solutions for health centres are described, which use the MSS as the service for a transaction that the user has initiated. The MSS in this thesis is based on authentication and on signature of plain text content or signature of a digest of a content. Tests of some proposed mobile certificate based services are also described.

1.3 Limitations

The mobile operators in Finland follow Finnish Federation for Communications and Teleinformatics (FiCom) recommendations, but each operator will determine the extent to which this occurs. The thesis follows FiCom recommendations and the European Telecommunications Standards Institute (ETSI) standards used in FiCom-recommendations. In this thesis some selected proposed mobile certificate based services are tested. There is also no technical description on how the MSS is created, because it remains outside of the scope of this thesis work.

2 MOBILE CERTIFICATE

The mobile certificate is an electronic identification token, which is used for authenticating the identity of a person and for approving a transaction or an agreement. Therefore it is used for granting access to electronic services and for digital signing of a text

or a document (Mobiilivarmenne, 2011a). The mobile certificate is stored in the SIM card with the owner's personal information and is provided by the operators (Mobiilivarmenne, 2011c).

The mobile certificate has been developed in Finland as collaboration between mobile operators (Mobiilivarmenne, 2010).

The mobile operators have also signed a trust network agreement as Certification Authorities (CA) and agreed on a certification policy, which they manage and update (Mobiiliasiointivarmenne, 2011:2). The certification policy is an outcome of an agreement between mobile operators to guide decisions, achieve rational and common outcomes (Mobiilivarmenne, 2010).

A mobile certificate can be created according to the FiCom recommendation document (FiCom. 2012b:5).

The mobile certificate is delivered or handed to the end user by making an agreement with the mobile operator (Mobiilivarmenne, 2011a). The end user will get a certificate based Subscriber Identity Module (SIM) card, for which a Personal Identification Number (PIN) is included (Mobiilivarmenne, 2011c).

2.1 FiCom recommendation

The FiCom recommendation is an application guideline document for the ETSI MSS standards. The mobile certificate can be realized with the techniques, practices, limitations and extensions implemented by various service providers in Finland. This is described in FiCom recommendation. The FiCom recommendation relies on ETSI TS 102 204, TR 102 206 and TS 102 207 standards. The FiCom recommendation is created by FiCom ry. (FiCom, 2012b:5)

The FiCom recommendation is based on the following techniques (FiCom, 2012b:5-6):

- XML Schema Part1; Part 2
- Soap Version 1.2 Part 0: Primer; Part1: Messaging Framework; Part 2: Adjuncts
- XMLSignature
- WSDL 1.1

- PKCS#7
- Security Assertion Markup Language (SAML) v2.0.

2.2 FiCom (Finnish Federation for Communications and Teleinformatics)

FiCom, Finnish Federation for Communications and Teleinformatics, is a Finnish Information and Communications Technology (ICT) sector trustee and cooperation organization. The members of FiCom are companies, which are telecom, Internet and cable operators and more. The members work with communications and the Teleinformatics sector in Finland. (FiCom, 2012a)

2.3 ETSI (European Telecommunications Standards Institute)

ETSI, European Telecommunications Standards Institute, is an European Standards Organization which produces globally applicable standards for (ICT). These standards are for mobile, radio, fixed, converged, broadcast and Internet Technologies. (ETSI, 2011)

3 MOBILE SIGNATURE

Mobile signature is an electronic signature that is considered and accepted as a handwritten signature. It is created by a user through a cryptographic process by equipment that is needed to create the signature. Therefore a mobile signature can be implemented in a variety of ways with the use of capabilities of a mobile device (SIM/UICC infrastructure) and mobile network infrastructures. (ETSI, 2003a:12)

The working definition for the mobile signature is described in an ETSI standard as follows:

> "A universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction" (ETSI, 2003a:12)

The mobile signature can be used in devices such as the mobile telephone, tablet computer, PDA, Laptop PC and remote telemetry unit with integral or external smartcards using a mobile network as a communications channel. (ETSI, 2003a:12)

The mobile signature can be enhanced by improving the protection against certain potential threats with the additional utilities such as “time-stamping” (i.e. describes the date and time at a given moment) and can be used to clarify that the transaction was made on behalf of the citizen’s request on a specific time. (ETSI, 2003a:12)

The mobile signature is used in services were the user has initiated and wants to grant the permission to proceed with a transaction. The service may be initiated through the Internet, voice-call, interactive voice response systems and other electronic communications channels. Therefore face-to-face services are also possible. (ETSI, 2003a:12)

3.1 Mobile Signature Design

The mobile signature functionality can be included in Server Side and Smart Card based implementations, which use any mobile network communication such as USSD, SMS, Circuit Switched, and GPRS as a communication channel. Even protocols like WAP can be used for signing, which then can be achieved by installing a suitable application in the mobile device that can be addressed by an application or service being used by the user. (ETSI, 2003a:13)

A server side signature creation is achieved with a signature “proxy” or “gateway” and the mobile signature is an encryption of an appropriate code such as Message Authentication Code (MAC). The signature is created by the server whenever the user has entered the PIN-code using the mobile device keypad. (ETSI, 2003a:14)

The smartcard based signature creation is achieved by a crypto processor, which can be implemented on a smartcard such as SIM-card and Universal Integrated Circuit Card (UICC). Therefore mobile operators have the role of “Smartcard Issuer”. (ETSI, 2003a:14)
A Mobile Smartcard Implementation is shown in Figure 1.

Figure 1 Typical Mobile Smartcard Implementation. (ETSI, 2003a:14)

The difference between the server side and the smart card based signatures is that the server side signature validity cannot provide as high degree of confidence as the smart card based signature. (ETSI, 2003a:14)

3.2 Cryptographic Techniques

Cryptographically, a user signs a document digitally with his/her private key. The user then creates a digital certificate that includes a hash encrypted with user's private key. The digital certificate can be verified with the user's public key. Therefore other parties can rely upon signatures made by the private key with the trust of the public key that is published for verification. (Roger R. Dube. 2008:132-133)

The cryptographic technique for creating a mobile signature can be asymmetric or symmetric (Roger R. Dube. 2008:132-133).

The asymmetric key technique uses different keys for encryption and decryption. The keys that are used are the private key and the public key. The private key is used for decrypting or signing the message and the public key is used to encrypt a message or verify a signature. The keys are linked mathematically, but with high complexity. (Roger R. Dube. 2008:2-3)

The symmetric key techniques use identical or related cryptographic keys, which are used for both encryption and decryption. If the keys are related then they can be made

identical by some transformation. Symmetric keys are also called shared keys or secret keys. (Roger R. Dube. 2008:2-3)

The difference between the asymmetric and symmetric keys is that the symmetric key has the advantage of faster computing, but is more vulnerable to security threats. (Roger R. Dube. 2008:2-3)

3.3 Public Key Infrastructure (PKI) Technology

A Public Key Infrastructure (PKI) is used for creating, storing and distributing digital certificates. A digital certificate connects an entity with a public key. A PKI needs both public key and private keys. Public keys are distributed and private keys are held secret and stored securely. Therefore a private key can be stored on a SIM or UICC card etc. (ETSI, 2003a:15)

In a PKI there are Registration and Certification Authorities for creating, issuing and revoking certificates. (ETSI, 2003a:15)

3.4 Technology Choice

To create a mobile signature, which is considered as an electronic signature, different technologies can be deployed. Smartcard (SIM or UICC) technology can be integrated in a mobile device and in any network node. (ETSI, 2003a:16)

Some mobile signature technologies are shown in Figure 2.

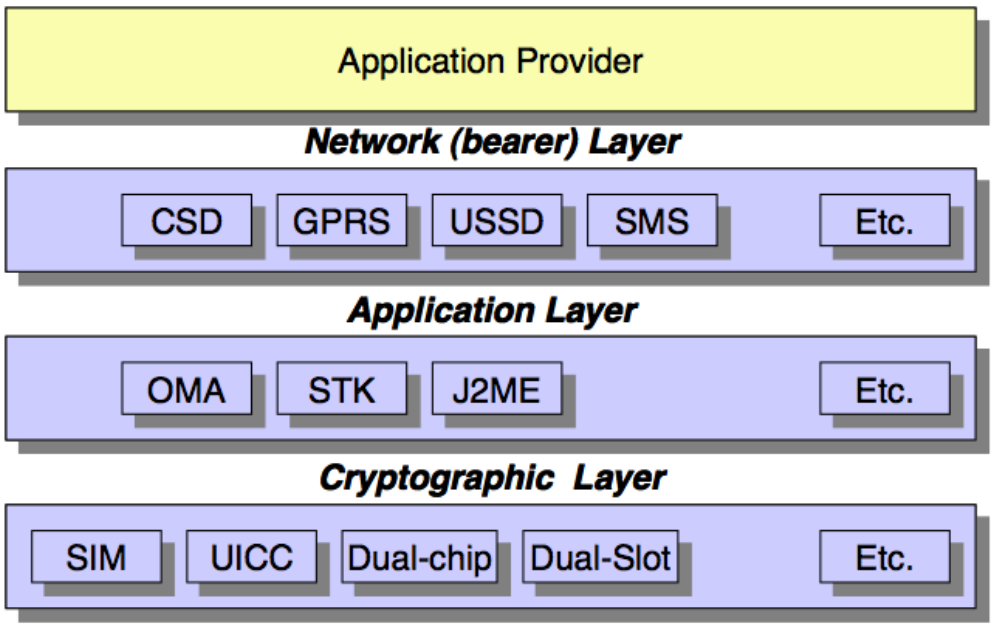

Figure 2 Modular Approach to Mobile Signature. (ETSI, 2003a:16)

3.5 Mobile Signature Service (MSS)

The MSS can be defined as a service for users and application providers, where the mobile signature process is coordinated or managed. (ETSI, 2003a:7)

The MSS is provided from MSSP to service providers. The role of MSSP is to execute registration and certification procedures. (ETSI, 2003b:12-13)

A MSS has a Web Service Interface, which MSSP provides and/or implements as a Mobile Signature Web Service between end users and AP. (ETSI, 2003b:13)

4 MOBILE SIGNATURE SERVICE PROVIDER (MSSP)

A MSSP distributes Mobile Signature Services to service providers with a high level of security. To provide such services there are only few procedures to execute for registration and certification.

The mobile PKI registration process needs four entities to be implemented. These are the Certification Authority (CA), the Registration Authority (RA), the MSSP and the end user. A MSSP may possess a CA and optionally a RA. (ETSI, 2003b:14).

4.1 Certification Authority (CA) & Registration Authority (RA)

In cryptography, a CA provides registered users digital certificates for their public keys. RA can process user information. A digital certificate is signed with CA's private key, which then indicates that the digital certificate is trusted by the CA. (ETSI, 2003a:41)

The CA acts as a Trusted Third Party (TTP) and the public key of CA is used for verification of the certificate carrying the user's public key. (Roger R. Dube. 2008:132-133)

The RA obtains and validates personal information provided from the users who want to use mobile signature services. Therefore there is a CA policy to be followed. This means that there is a certification policy and certification practice declaration. The RA also issues a certificate for a user's public key. (ETSI, 2003a:41)

The MSSP in Finland acts as a CA and as a RA. (Mobiiliasiointivarmenne, 2011:12-13)

4.2 Mobile Signature Profile

A Mobile Signature Profile proves some kind of signature quality to the AP, based on mobile signature capabilities.
MSSP will provide a Mobile Signature Profile to the AP, which the AP uses whenever requesting a Mobile Signature. The Mobile Signature Profile is used with a Uniform Resource Identifier (URI) pointer. Therefore both parties can define their own URI's by any appropriate means. (ETSI, 2003b:14)

4.3 Mobile Signature Messaging Modes

There are two messaging modes, "synchronous" mode and "asynchronous" mode, for achieving a mobile signature. In this chapter, the concept "MSSP" generally refers to

the system utilizing signature service roaming, formed by all operators. When trying to invoke the end-user mobile device for confirmation of a transaction there are steps that may take a while, such as which is network connection etc. Therefore the best transaction processing mode for MSSP would be "asynchronous". A multi request-response protocol is needed from the MSSP to get the "asynchronous" mode function properly. (ETSI, 2003b:15-17)

Below is a description of the "Asynchronous Client-Server" and "Synchronous Client-Server" communication modes that are supported in the FiCom recommendation. The messaging communication modes have following service messages: signature request, related signature response, status request and related status response. There are also additional and optional service messages, which are receipt request and a related receipt response. The messaging modes are used for AP to request and receive related response from the AE. (FiCom. 2012b:9)

The signature request message mode is for requesting signature from an AE. AP then requests it from the user through the HMSSP (FiCom. 2012b:14). The signature response message mode is for acquiring a signature response from an AE. AE sends the signature response to AP as an acknowledgment of the signature request (FiCom. 2012b:31).

The status request message mode is for inquiring from an HMSSP the completion of the previously submitted service request (FiCom. 2012b:40). The HMSSP reports the status of the signature event in the status response message mode. (FiCom. 2012b:42)

The receipt request message mode is for sending an acknowledgment of the success or failure of the event to the user (FiCom. 2012b:44). The receipt response message mode is for acquiring the requested acknowledgment is sent. (FiCom. 2012b:47)

The messaging modes use many HTTP events, which follow each other and are established in the AP's system. The messaging modes are useful for obtaining reference in-

formation about asynchronous communication at an early stage and therefore give high service reliability. (FiCom. 2012b:9)

4.3.1 "Asynchronous – Client-Server" Mode

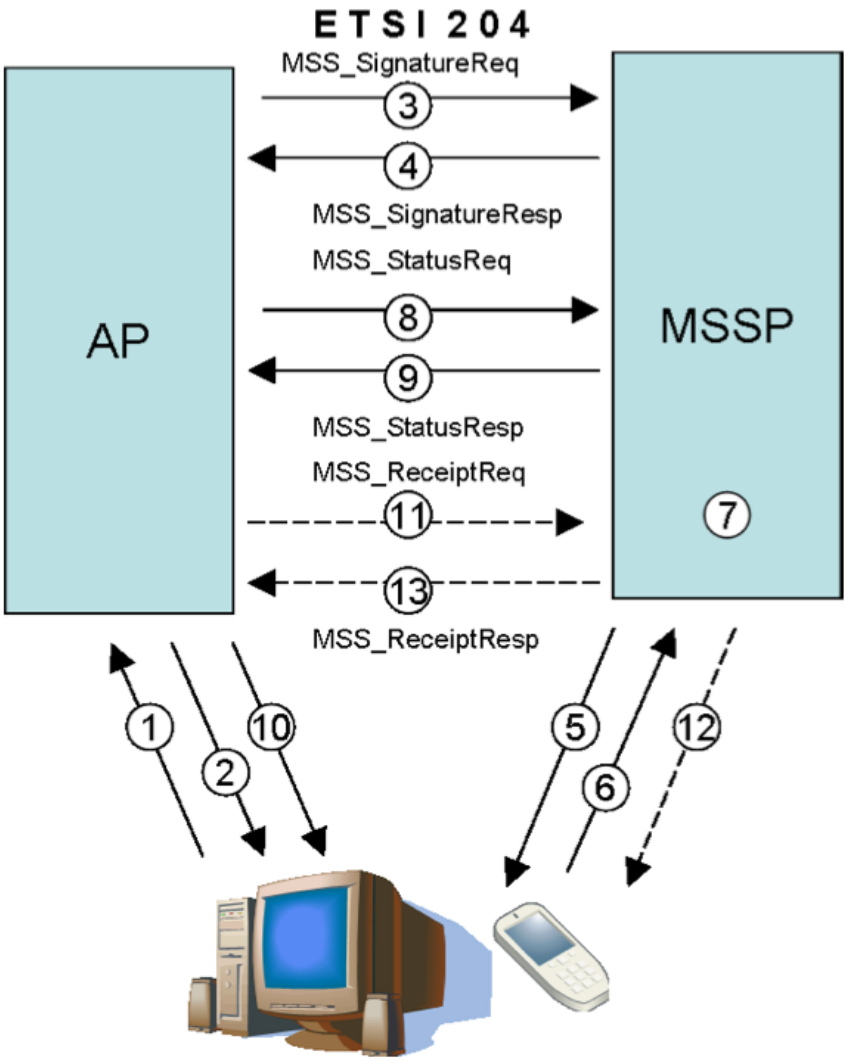

Figure 3 Signature Method – "Asynchronous Client-Server" Mode. (FiCom, 2012b:10)

1. The user establishes a connection to AP's server. The user wants to access a service or sign an electronic text or document. Therefore the AP server asks the user for information such as mobile phone number and spam prevention code (SPC).

2. The AP server displays the event number in the current business channel that identifies the signature event and guides the user to look on the device (mobile phone).
3. The AP server can now request a signature from an Acquiring Entity (AE), with which the Web Service Interface has been integrated. There is a mutual authentication between the AP server and the AE. The request can also include additional information of the user's identity, which the AP server may ask from Home Mobile Signature Service Provider (HMSSP).
4. When the signature request is received an MSSP event number is generated and the AE returns the event number to the AP server and a description of the event is indicated in the response message.
5. The AE makes sure that the information, which was requested, is in accordance with the service agreement. Afterwards the AE sends the message to the user's HMSSP, which is the user's operator. The HMSSP invokes the user's mobile phone for signature request if the user's SPC is correct and the user allows the signature service (incl. value-added services) to be requested by the AP server.
6. The user gets a signature request, which also shows the same event number that was shown in the AP server interface and therefore the user has to ensure that both correspond to each other. Afterwards the user can sign the event by inputting the given PIN code. The result is a digital signature, which is delivered to the HMSSP.
7. The HMSSP creates a PKCS#7 message by compiling a digitally signed message from the digital signature. This message is then attached as a part of to the signature response (MSS_StatusResp). The value-added service, which was requested from the AP server will also be processed and attached to the digitally signed message.
8. After the AP server has sent the signature request to the AE to be processed, the AP server asks for the completed signature response at specified intervals (MSS_StatusReq).
9. The HMSSP verifies the digital signature and reports the status of the signature request in the status response (MSS_StatusResp) to the AP server's (MSS_StatusReq). The completion of the signature is delivered as part of the status response.

10. The AP server links between the User identified in the signature response (a digital signature) and the one with the AP server's own database. When the AP server has identified the User, the result of the process is called authenticated. Therefore the AP server's interface can be changed to an authenticated interface.
11. When the AP server has been assured of User's identity, it can send a receipt of the completion of the event to the User through the same channel, which was used during the signature request, but using the receipt request instead (MSS_ReceiptReq).
12. The receipt message request is delivered to User.
13. The response of the receipt is delivered the same way as the signature response (MSS_ReceiptResp). (FiCom, 2012b:10-11)

4.3.2 "Synchronous Client-Server" Mode

The only difference in "Synchronous Client-Server" compared to the "Asynchronous Client-Server" messaging mode is that the connection is established until the signature response is acquired from HMSSP to the AP server and therefore the MSSP sends the signature response to the AP server. (ETSI, 2003b:15)

This messaging mode is not recommended by FiCom, because of it consumes system resources of the AP server and the MSSP unnecessarily (FiCom, 2012b), but ETSI declares that this messaging mode has to be supported by the MSSP (ETSI, 2003b:15).

5 APPLICATION PROVIDER'S INTERFACE

5.1 General Message structure

The message interface between AP and AE is created in the form of MSS service messages, which are described by ETSI (ETSI, 2003b:21-23).

The AP sends a service request to the AE and receives a related service response. The service request of AP is a HTTP POST Request and the AE's response message is a HTTP Response. The MSS Service messages are included in SOAP envelopes, which

are transmitted as HTTP messages. A SOAP envelope contains a header element (env:Header) and a content element (env:Body). (FiCom, 2012b:11)

5.2 SOAP Header

The Header element in SOAP is optional. It is useful for implementing XML signatures, which the FiCom recommendation does not address. (FiCom, 2012b:11)

5.3 SOAP Body

The Body element in SOAP is compulsory and one of the following message types is attached to it (FiCom, 2012b:11):

- MSS_SignatureReq (operation: MSS_Signature)
- MSS_SignatureResp (operation: MSS_Signature)
- MSS_StatusReq (operation: MSS_Status)
- MSS_StatusResp (operation: MSS_Status)
- MSS_ReceiptReq (operation: MSS_Receipt)
- MSS_ReceiptResp (operation: MSS_Receipt)

Each message type includes further attributes and sub-elements specific to the message type. The Web Service Description Language (WSDL) 1.1 specifies that the message element is covered inside the element specifying the name of the “operation”. (FiCom, 2012b:11)

5.4 Namespaces

The element specifying the SOAP Envelope reserves its own namespace (FiCom, 2012b:12):

<env:Envelope xmlns:env=”http://www.w3.org/2003/05/soap-envelope”>

The element specifying the message type of the content element reserves namespaces for the ETSI MSS standard specifications and if necessary for specifications of the

XML signature and for value added services of signature requests specified by the FiCom recommendation:

<MSS_ReceiptReq xmlns=http://uri.etsi.org/TS102204/v1.1.2#
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:fi="http://mss.ficom.fi/TS102204/v1.0.0#" ...>

Several examples of each MSS service message are presented in the FiCom recommendation. An example of a general message structure is presented below. (FiCom, 2012b:12):

```
POST /MSS_Signature HTTP/1.0
Host: mss.teliasonera.com
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...
<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
<!- Optional header -->
<env:Header>
</env:Header>
<!- Mandatory body -->
<env:Body>
<-! WDSL op name -->
<MSS_Signature>
<!- MSS service message -->
<MSS_SignatureReq ...>
...
</MSS_SignatureReq>
</MSS_Signature>
</env:Body>
</env:Envelope>
```

5.5 Not addressed message types

The following MSS standard message types are not addressed by the FiCom recommendation:

- MSS_RegistrationReq
- MSS_RegistrationResp
- MSS_ProfileReq
- MSS_ProfileResp
- MSS_HandshakeReq
- MSS_HandshakeResp

5.6 Error handling

On error during of an event, a SOAP FAULT message is returned to the Application Provider. The SOAP FAULT message contains a status code of the error.

6 MOBILE CERTIFICATE BASED SERVICES

The mobile certificate can be deployed in health centre services, from which healthcare personnel (administrative personnel, nurses, physicians and dentists) and health centre users benefit. This section proposes mobile certificate based services for health centre users and personnel.

6.1 Healthcare User

Below is a description of different ways of using mobile certificate network services through a web interface, with SMS, or during a phone call. All Mobile Signature based Services described below use the web interface to activate the Mobile Signature Service (described in subsection 4.3.1.).

According to ETSI standards that are used in the FiCom recommendation the services that are described below can be created with additional information from the user. This additional information is the mobile phone number and SPC or user ID instead of mo-

bile phone number. The user ID acts as a mobile phone number. Whenever the user ID is used the server will search the corresponding user ID in the database and use the mobile phone number that was registered with that user ID. This means that the database has to be updated, whenever the user changes the mobile phone number.

6.1.1 Authentication when accessing health centre's website

The user tries to log in with a computer or a mobile device to the health centre's webpage. The user has to authenticate himself/herself with the mobile certificate to be able to use services. The web page offers the users various services such as access to Espoo's self care Health file (Espoo, 2012), KanTa – the National Archive of Health Information (KanTa, 2009), and other electronic services which need authentication.

Espoo's self care Health file is an electronic service that allows the user to interact with a physician and a nurse online. The user can also have a personalized treatment plan, which can be updated with a notification to a physician or a nurse. (Espoo, 2012)

KanTa – National Archive of Health Information is a national medical information system including (KanTa, 2009):

- Electronic Prescription (ePrescription) and the National Pharmaceutical Database
- Electronic Archive of Patient Records (eArchive)
- Access to personal prescription and medical data

6.1.2 Confirmation of a reservation

The user wants to reserve an appointment time with a physician, dentist or nurse from a web page. In the webpage the user chooses the details of the appointment such as time, date, health centre, physician, dentist or nurse. Therefore a signature request will be sent to the user's mobile phone for confirmation. The signature request is a commitment with appointment details. This commitment is described below.

6.1.3 Signing a commitment

The user wants to sign a commitment to agree or to give permission. The commitment can be a contract, a document, an e-mail message or some other text, which needs to be signed.
The user selects the commitment that needs to be signed from a webpage. Therefore the user's mobile phone will be invoked, which describes the need of signing a commitment for the health centre.
The user checks if the current commitment corresponds with the one the user selected in the health centre's webpage, if they match the user signs with the PIN-code.

6.1.4 Proof of identity

Proof of identity can be used on such occasions where users have no other way to prove their identity. This means that a user is strongly authenticated by using the mobile certificate for identifying himself/herself for the health centre's staff member. It can also be used to allow a physician, dentist or nurse to have access to a patient's record, even when the person is not present in the health centre. This can be achieved by setting the need for authentication whenever the physician, dentist or nurse needs access to the patient's records. Therefore, for example, there should be certain rules for cases when there is no need for authentication, such as:

- Acute occasions, when a patient is in bad condition and may die or surgery is urgently needed (There could be the patient's family relative who can give the permission by authentication with the mobile certificate)
- The same day when the user has appointment with the physician, dentist or nurse
- Other possible cases

The user gives his/her mobile phone number or user ID with the predefined SPC code to the health centre staff member. The staff member urges the user to authenticate with his/her mobile certificate. To prevent the eavesdropper to hear the SPC code when the user wants to proof his/her identity, the SPC can be predefined in the health centre's

user database. Then the SPC will be used from the database without needing the user to inform the SPC to the health centre's staff member.

6.1.5 Payment

A health centre's bill can be paid from the health centre's web page. The staff member asks the user if the payment will be made with credit cards or through the health centre's web page when visiting the physician, dentist or nurse. If the user wishes to pay from the web page, the staff member puts the bill on the users account. Therefore the user needs to have an account.

The user authenticates himself/herself when accessing his/her account. The user selects the bill from his/her account and pays with mobile certificate through the banks web interface, which has been integrated in the health centre's web page. This service needs agreement with the bank and also the mobile certificate payment method has to be provided by the bank.

6.1.6 Anonymous authentication

Control of a user's age or gender can be implemented in order to provide access to information relevant to a particular age or partial gender. An example is displaying pictures or disease images to which an adolescent should not have access.

Verification service can also be used anonymously to publish statistics on how many men and women have answered a certain question or when a user comments a webpage and also for voting on an answer of a question. Therefore this feature uses only some information from the mobile certificate. (FiCom, 2012b:8)

6.1.7 Registration for SMS-services

In health centre SMS services, which need registration and authorization, the mobile certificate can be used to ensure that the user wants to use the SMS service.

A User wants to register for an SMS service, which the health centre provides. The user sends an SMS message to the health centre's SMS service registration number. The message contains the user's mobile phone number, SPC and the name of health centre's SMS service.
The user receives a text message with an event number, the service the user chose and a deadline for mobile certificate service activation. The user's mobile phone will be invoked for signing, which shows the user, the event number, and the name of the health centre's SMS service that the user wants to register for. The user checks if the event number corresponds with the described event number in the SMS message and signs with his PIN to register for the SMS service.

6.1.8 Time reservation with SMS

In reserving an appointment with a physician, dentist or nurse SMS can be used as a communication channel for reserving the time. The user signs a confirmation of the reservation with the mobile certificate.

The user makes an appointment by sending to a specific number an SMS with additional details for example such as reason, social security number, date, time, physician, dentist or nurse.
The server checks if the requested reservation time is occupied. If not, an SMS is sent back to the user for signing the reservation with the mobile certificate. If the requested reservation time is occupied the user receives several alternatives by SMS. The user can choose and confirm a suitable alternative. Therefore an SMS is sent back to the user for signing the reservation with the mobile certificate. The SMS contains information such as the event number, the reservation ID and the deadline for mobile certification activation.

The user's mobile phone will be invoked for confirmation by signing with the mobile certificate. The user checks if the event ID and the reservation ID or the displayed text, which describes the reservation details, is correct and signs with his/her PIN.

6.1.9 Strong authentication of identity during a phone call

During a call, the user authenticates himself/herself to allow a health centre staff member to provide services. This service uses a web page where the staff member inputs the user's mobile phone number and SPC for authorization. The health centre staff member informs the user the event ID, which will be used during authentication of the user with the mobile certificate.

Once the user has authenticated himself/herself the health centre staff member can offer various services such as booking, rebooking, cancellation of the reservation, change of registered information and more.
In addition, to the user can be sent a confirmation, which describes the service that was used and the changes that were made. The user accepts the confirmation by signing it with the mobile certificate.

6.1.10 Signing a commitment during a phone call

Signing a commitment, which is a contract or a document that a health centre staff member will describe to the user during a telephone conversation. This service may be required in circumstances such as using a particular service or the health centre must have parental permission for surgery on a child or other related dependencies. This service uses a web page where the health centre staff member chooses a contract or a document to be signed by the user using the mobile certificate.

The user agrees with the health centre staff member to sign a contract or a document during a phone call. The health centre staff member asks and inputs the mobile phone number and SPC from the user into the contract or document. The health centre staff member informs the user through the phone, the event ID and the name of the document or contract that needs to be authorized. Therefore the user checks if the details are correct and signs with his/her mobile certificate.

The staff member is responsible to the user for any untold information, which can lead to misunderstanding. Therefore the conversation between the staff member and the user should be recorded for further use.

6.1.11 Confirmation of information change during a phone call

This service can be used as an additional confirmation from a user for example where the user changes contact details, or other related services as described in subsection 6.1.9. This means that the changes, which were made were authorized by the user and in this case there will be no mistyping or misunderstanding.

A confirmation of changed contact details or other related service can be signed for confirming the change immediately. If the changed information is correct, the user signs the changed details with his/her mobile certificate.

6.2 Healthcare Personnel

In this section staff refers to administrative persons, physicians, dentists or nurses.
A staff ID, which is mentioned below is an ID that can be used when a staff member tries to log in. A staff member works in general as a user ID, but the staff ID is a link to the staff member's mobile phone number. Therefore both staff ID and mobile phone number has to be registered and updated in the staff database.

6.2.1 Authentication when accessing health centre's website

A staff member tries to log in with a computer or a mobile device to the health centre's webpage by authenticating himself/herself. The web page provides the health centre staff member's services such as access to Espoo's self care Health file (Espoo, 2012), KanTa – the National Archive of Health Information (KanTa) or other electronic services, which need authentication.
Espoo's self care Health-file (Espoo, 2012) and KanTa – the National Archive of Health Information (KanTa) are described in the subsection 6.1.1.

6.2.2 Signing documents, recipes, e-mail or agreements

A staff member signs a document such as a PDF file, an e-mail message, or a contract. A physician can additionally renew or modify a recipe and sign the recipe to make it approved immediately.

Examples:

- Signing changes that must take place in the health centre and must have staff member’s approval (e.g. health centre’s policy).
- Renewal of a prescription that a patient has requested.
- Staff members can also sign their employment contracts or other agreements that need to be signed.

6.2.3 Access to fileserver

Staff members authenticate themselves with the mobile certificate to get access to a file server. The file sever is an File Transport Protocol (FTP) server and can be accessed through an web interface where the staff member can upload or download files etc.
This service can be used for transmission of files and for distance information on such occasions where staff members are not present or even might need to update software to be able to use it again.

6.2.4 VPN connection

A staff member can log on to the health centre's intranet using a Virtual Private Network (VPN) connection. A VPN connection can be opened using a mobile certificate as an authentication method. Staff members who are not present, but need to use the intranet services or files, can use this service.

A staff member establishes a VPN connection to the health centre's internal network with the VPN client application, which then activates the mobile certificate for authentication. The staff member authenticates and gets access to intranet services.

7 IMPLEMENTATION OF MOBILE CERTIFICATE BASED SERVICES

Below is an outline of how to solve the network, phone call or SMS services. The phone call or SMS services are implemented using the network service. The FiCom recom-

mendation and the Laverca Software Development Kit (SDK) are also described and how these are utilized to get the mobile certificate service function properly.

7.1 FiCom recommendation in brief

To understand the potential of how the Mobile Signature Service works in practice there is need of familiarization with the described techniques used in FiCom recommendation v2.1 (described in subsection 2.1.1.) and ETSI's MSS standards.

The currently supported messaging modes are asynchronous client – server and synchronous client – server (not recommended). The asynchronous server – server messaging mode is currently not supported. Strong mutual authentication and encryption is used between all entities contributing to the routing of the message. (FiCom, 2012b:8)

An agreement between the AP and AE is needed to get access to a mobile certificate service. Once an agreement has been made with the AE additional information will be provided. (FiCom, 2012b:8):

- AP name (Application Providers name):
- The AP name is displayed on the terminal device
- AP_ID (Application Provider ID) & AP_PWD (Application Provider Password):
- The AP_ID and AP_PWD are used as an addition to strong mutual authentication and encryption between AP and AE

The list below describes the FiCom recommendation in brief (FiCom, 2012b:8):

- Currently supported message formats are MSS_SignatureReq, MSS_SignatureResp, MSS_StatusReq, MSS_StatusResp, MSS_RecepitReq, MSS_ReceiptResp.
- The process of the user registration is an internal matter for each HMSSP.
- The MSS Service registration messages are not addressed in this version of recommendation.
- XML signed service messages are currently not supported.
- The MSISDN is used for finding the user and HMSSP.

- A user can be also found with the UserIdentifier whose mandatory postfix additionally identifies HMSSP, but is currently not supported.
- The supported character sets in service requests are GSM, UTF-8 and UCS2.
- The supported character sets on a terminal device are GSM 03.38 and UCS2.
- Only the UTF-8 characters are available and included in the GSM 03.38 character set.
- The HMSSP provides six different signature services:
- Authentication
- Anonymous Authentication (currently not supported)
- Signature of plain text content
- Signature of digest content (currently not supported)
- Issuing consent
- Operator service for authentication
- Each HMSSP signature service is a separate signature profile, which indicates the desired service.
- The users can prohibit signature profiles through his/her own mobile subscription.
- AdditionalServices is an added value service used as an expansion for the MSS standard:
- Mobile phone spam prevention (SPC)
- An event ID
- AE validation (currently not supported)
- User's language preference (currently not supported)
- PersonIdentity service
- The format of the signature requests is standardized.
- The user's certificate is supplemented with a digital signature format base64-encoded PKCS#7 or PKCS#1 (currently not supported).
- It is mandatory to synchronize the system clock for AE, RE, and HMSSP with the NTP service. It is also recommended for AP.

7.2 Laverca SDK

The Laverca SDK is a Mobile Signature Service Application Programming Interface (MSSAPI), which is an Open Source implementation of ETSI TS 102 204 client software in Java. In addition to the ETSI standard it also supports the FiCom recommendation functionality and the developer does not need to be familiar with the asynchronous client – server messaging mode operating principle. (Sourceforge, 2011)

7.3 Network service

In order to implement mobile certificate based network services, the following is needed:

- Web server with a platform (Linux, Windows)
- Certificate (server certificate)
- Access to patient records (KanTa, Espoo's self care healthfile)
- Database (Staff, Users)
- Agreement with the AE
- Secure communication between all parties

A server that acts as a web server with installed operating system (Linux or Windows) is required. The web server can be installed using open source software or license based web server software such as Apache or Microsoft IIS (Internet Information Services). A server certificate is needed for using the mobile certificate service for authentication and for encryption of the communication between AP and the AE server (mutual authentication). In addition, the server certificate is used for encryption when clients visit the web page (user). The certificate must be installed on the server side. The server must also have access to patient records to manage user information. The server must also have access to a database that contains information of the health centre's staff members and users. This database is needed for identifying the mobile phone number from an ID in authentication with a mobile certificate. The authenticated user is linked with the health centre's database.

An agreement with the operator is needed for setting up a mobile certificate based service. Once an agreement has been made with the operator additional authentication information will be provided (sourceforge, 2011):

- AP name (Application Providers name)
- AP_ID (Application Provider ID)
- AP_PWD (Application Provider Password)
- MSS_Signature URI (Operator's Signature request Uniform Resource Identifier)
- MSS_Status URI (Operator's Status request Uniform Resource Identifier)
- MSS_Receipt URI (Operator's Receipt request Uniform Resource Identifier)

The additional authentication information is used for establishing a connection to the operator's server and using the appropriate MSS-service URI for sending a SOAP envelope as an HTTP message (Sourceforge, 2011).

Data communication between the parties is encrypted and also secured by mutual authentication. To implement the mobile certificate services according to FiCom recommendations for data communication the MSS standard must be used. (Sourceforge, 2011)

A MSS service message sent to the operator is based on a HTTP POST request and the related response from the operator is based on the HTTP response, which is described in section 5 (FiCom, 2012b:11).

The communication method that is used can be asynchronous client-server or synchronous client-server (not recommended) (FiCom, 2012b:8).

7.3.1 File Transport Protocol (FTP) server

Implementing the subsection 6.2.3, there is need of an FTP server. The FTP server can be accessed through a Web Interface. The Web Interface uses the Network service described above for authentication.

7.4 Virtual Private Network (VPN) service

Implementing the subsection 6.2.4, there is need of a VPN server. The VPN server must have access to the Health centre's database for verification of the users (health centre's staff members). There is also need of a VPN client for the user to connect to the VPN server. The VPN client can be custom created or by running a script for authentication with a mobile certificate. This service can also be implemented by a company, which solves is specialized in this type of solution. Therefore different approaches can be used.

7.5 SMS service

SMS services described in subsections 6.1.7 and 6.1.8 are like network services, but also need an SMS Gateway server connected to the health centre's web server. An SMS Gateway server waits for incoming messages and accepts only information such as the described information used as an SMS in the subsections 6.1.7 and 6.1.8.
The SMS Gateway server sends an SMS to the user in response to the service being used by the user. This is also described in the subsections 6.1.7 and 6.1.8. Therefore a SMS Gateway server creates a separate HTTPS event (HTTPS request) in the health centre's web server. The HTTPS event uses the information that was obtained from the SMS service and requests a signature from the user with the mobile certificate. The request can be a text or an ID that describes the service used by the user. The health centre's web server can verify if the correct ID or text was signed by the user and therefore process the user's request.

7.6 Phone Call Service

Phone call services described in subsections 6.1.9, 6.1.10 and 6.1.11 use the network services as an web interface for authentication of the user. Health centre staff members connect with their browser to the internal website and enter the health centre user's mobile phone number and SPC code. The staff member informs the user about the event number that will be used for authentication. The user checks if the given event number corresponds with the displayed event number in the mobile device. The user signs and the staff member will have access to the user's information and therefore can provide

services. In addition, a confirmation of the service used and the changes made can be signed by the user using the mobile certificate.
The following can be considered for preventing confidential information to be accessed by staff members:

- The Graphical User Interface (GUI) can be customized to the service used by the staff member and requested by the user.
- The SPC can also be predefined in the database as the user ID for activation of a mobile certification service.

8 TEST CASES

8.1 Introduction

This section describes the selected test cases that were tested partly or fully.
The following software and development kits were needed to run the test cases:

- Eclipse Integrated Development Environment (IDE) framework V3.7.1 indigo
- Java Development Kit Standard Edition (JDK SE) V1.7.0_03
- Laverca V1.01 SDK
- Apache ant V1.8.3
- Bash script
- Java Server Page
- Ubuntu server V11.10
- Apache Tomcat V7.0.26

Eclipse was used for development of Java applications with the utilization of Laverca SDK. The Java JDK SE and Apache Ant were used for compilation of Java applications. The bash script was used for running Java application.

The test cases were designed with Java Server Page (JSP), which makes it possible for the software developers to create dynamically generated web pages based on HTML, XML or other types of document. JSP uses the Java programming language. Whenever the JSP page is visited for the first time, the server will compile the JSP file and then

run it. Each test case executes a bash script within the JSP. Then the bash script runs a Java application.

As a test server the operating system Linux (Ubuntu server V11.10) and the Apache Tomcat v7.0.26 were installed. Apache Tomcat supports web applications.

A description on how test cases were designed is included in this section. The test cases are authentication and signing text content.

8.2 Limitations

Because the FiCom recommendation does not support all signature services the signature of content digest was not tested, although this signature service was included in the selected test cases. The SMS Services presented in this thesis were also not tested due to time shortage. The code of the finished test cases is not published. Therefore only explanations on how the test cases were created are given. These explanations include how mobile certificate authentication and signing a text are implemented.

8.3 Authentication – Test case

With preinstalled correctly configured software, authentication can be achieved. To create this test case, three JSP pages following each other were needed. The first one is a page containing an HTML form, which redirects the user to the second JSP page when the user has submitted the mobile phone number and SPC.

The second JSP page uses the request.getParameter(“name”) command for reading the attributes mobile phone number and the SPC which the user submitted to the first JSP page. To be able to use the user input in the last page, which is the third JSP page, there is a need to execute the session.setAttribute(“key”, value) command for both attribute.

In the second JSP page a sequence number is generated with the System.currentTimeMillis() command and this number is used as an application provider transport ID (APtransID). There is also an event ID (eventID) shown to the user on the

JSP page. The application provider can create the eventID differently. The eventID was created by shortening the APtransID to the last 4 digits and adding a letter before the first digit. There is also a need of an "if statement", which will redirect the user to the third JSP page if the user has inputted the mobile phone number and SPC with the correct syntax.

The third JSP page uses the InputStreamReader and BufferedReader classes in Java for reading line by line the system output and for getting user information such as the user's name, electronic service ID or other related information of the user. This information is asked during a signature request.

The InputStreamReader class is used within the try catch method. The try catch method uses the session attributes from the second JSP page and executes the command. The command can either run directly the Java application or use a bash script that executes a Java application. Both use the mobile phone number, the SPC, the eventID and the APtransID as parameters. Due to security reasons, a bash script was used for hiding the path of the classes and the Java file.

The Java application takes 4 arguments, which are the ones used by the bash script.
To be able to authenticate the user, access to the operator's mobile certificate service is needed. This is achieved by acquiring a server certificate, AP_ID, AP_PWD, MSSP Signature Uniform Resource Identifier (URI), MSSP Status URI and MSSP Receipt URI.

The server certificate is used for mutual authentication and encryption. The SSL/TLS support is based on the Java Virtual Machine's standard support. The "keystore" and "truststore" files are used by the Java Virtual Machine. Both are Java keystore files. The "keystore" file holds a private key and a server certificate. The private key and server certificate are created when an agreement with the operator is made. The "truststore" file holds the operator's server certificate, which is publicly published.

The AP_ID and AP_PWD are used as an additional authentication for a signature request.

The location of the Java “keystore” and “truststore” files are defined in the Apache XML configuration with the specified password for accessing these Java keystores. The MSSP Signature Uniform Resource Identifier (URI), MSSP Status URI and MSSP Receipt URI are also defined in Apache XML configuration file, which the Java application will use when making the appropriate request for signature, status or receipt.

An example of how authentication can be achieved is illustrated below. A description document is included in the Laverca 1.01 software development kit (Sourceforge, 2011):

Importing the fi.lavera and org TS102204.v1_1_2.Service class files for authentication.

```
import fi.laverca.*;
import org.etsi.uri.TS102204.v1_1_2.Service;
```

The following variable values will be provided from AE when AP has made an agreement with the AE:

```
String apId  = “AP_ID”;
String apPwd = "AP_PWD";
String sigUrl = "MSSP Signature URI";
String statUrl= "MSSP Status URI";
String statUrl= "MSSP Receipt URI";
```

Creating the client FiComClient for requesting MSS.

```
FiComClient fiComClient = new FiComClient(apId, apPwd, sigUrl, statUrl, recUrl);
```

The User’s mobile phone number example +358123456789.

```
String phoneNumber = “+358123456789”;
```

The User’s Spam Prevention Code (SPC), which always begins with a letter.

```
String nospamCode = “A123F2”;
```

Generating a unique id for this transaction.

```
String apTransId = APtransID;
```

Generating an authentication challenge using the apTransId created in the JSP page.

```
Byte[] challenge = new DTBS(apTransId, DTBS.ENCODING_UTF8).toBytes();
```

Generating a unique id for this transaction.

```
String eventId = eventID;
```

The nospam service for the parameter SPC is created as a string. If the SPC is given, then the second parameter is true, otherwise it is false.

```
Service noSpamService = FiComAdditionalServices.createNoSpamService(SPC, false);
```

Creating an event ID service with the event ID.

```
Service eventIdService = FiComAdditionalServices.createEventIdService(eventId);
```

Additional information can be requested from the user by creating a linked list that holds the additional attributes in string format.

```
LinkedList<String> attributeNames = new LinkedList<String>();
    attributeNames.add(FiComAdditionalServices.PERSON_ID_GIVENNAME);
    attributeNames.add(FiComAdditionalServices.PERSON_ID_SURNAME);
    attributeNames.add(FiComAdditionalServices.PERSON_ID_SATU);
```

To be able to create the additional attributes the method createPersonIdService in FiComAdditionalServices class has to be called and also added to the linked list, which holds the person ID service.

```
Service personIdService =
FiComAdditionalServices.createPersonIdService(attributeNames);
    additionalServices.add(personIdService);
```

For user authentication the method authenticate in FiComClient class is used and the additional services could be added instead of the null parameter.

```
try {
   FiComRequest req = fiComClient.authenticate(apTransId,
                                    challenge,
                                    phoneNumber,
                                    noSpamService,
                                    eventIdService,
                                    null, // instead of null the additionalServices can be used
                                    new FiComResponseHandler() {
      @Override
      public void onResponse(FiComRequest req, FiComResponse resp) {
        log.info("got resp");
         System.out.println( “Signer: ”resp.getPkcs7Signature().getSignerCn());
      }
      @Override
      public void onError(FiComRequest req, Throwable throwable) {
         log.info("got error", throwable);
      }
      @Override
      public void onOutstandingProgress(FicomRequest req, ProgressUpdate prg) {
         log.info(“got progress update”);
      }
   });
}
catch (IOException e) {
}
```

The following code can be used for additional services in the override method onResponse of the FiComResponseHandler (illustrated above) class:

```
String line = "";
        List<FiComAdditionalServices.PersonIdAttribute>attributes=
resp.getPersonIdAttributes();
        for(FiComAdditionalServices.PersonIdAttribute pidAttr:attributes){
        if(pidAttr.getName().equals(FiComAdditionalServices.PERSON_ID_GIVENN
AME)) {
        line += " GIVENNAME= " + pidAttr.getStringValue();
        }
        if(pidAttr.getName().equals(FiComAdditionalServices.PERSON_ID_SURNAM
E)) {
        line += "\n SURNAME= " + pidAttr.getStringValue();
        }
        if(pidAttr.getName().equals(FiComAdditionalServices.PERSON_ID_SATU)) {
        line += "\n SATU= " + pidAttr.getStringValue();
        }
System.out.println(line);
```

8.4 Signing text – Test case

This test case was created in the same way as the authentication test, which is described above and it uses authentication test as a template. Therefore only some part is changed and will be described here.

The first JSP page can be created individually or be combined it with the authentication test case.
If created individually, the first JSP page contains a form with input fields for mobile phone number, SPC and text area. The additional text area is attached to the form.
If combined with the authentication test case, the first JSP gets the values of mobile phone number and SPC from the third JSP page of the authentication test case. The mobile number phone and SPC can be obtained using the session.setAttribute("key", value) command on the third JSP page of the authentication test case. The additional text area is also attached to the form. This means that there are five JSP pages following each other.

The text area mentioned above is used for signing and allows a maximum length of 160 characters.

The second JSP page saves the user's inputted text in the text area to a text file with the format ISO-8859-1. The text file will be used within the Java application.
The third JSP page will execute a bash script, which executes the Java application in the same way as in the authentication test case.

The Java application uses the following code to read a file in a ISO-8859-1 format:

```
StringBuilder text = new StringBuilder();
String NL = System.getProperty("line.separator");
Scanner scanner = new Scanner(new FileInputStream("TEXT_FILE"), "ISO-8859-1");
        try {
        while (scanner.hasNextLine()){
        text.append(scanner.nextLine() + NL);
        }
        }
        finally{
        scanner.close();
        textToBeSigned = text.toString();
        }
```

Only the additional service attribute name PERSON_ID_VALIDUNTIL is used for controlling the validity of the user.

```
attributeNames.add(FiComAdditionalServices.PERSON_ID_VALIDUNTIL);
```

The method signText in fiComClient class is used for signing requests with the same parameter as in authentication test case, but only the parameter challenge is changed to a string variable textToBeSigned, which is the text to be signed by the user and is obtained from the text file.

```
fiComClient.signText(aptransID,
                                textToBeSigned,
                                phoneNumber,
                                noSpamService,
                                eventIdService,
                                additionalServices,
                                new FiComResponseHandler() {
                                        @Override
                public void onResponse(FiComRequest req, FiComResponse resp) {
                log.info("got resp");
                try {
                System.out.println("Signer: " + resp.getPkcs7Signature().getSignerCn());
                System.out.println ("MSS Signature: " + new
String(Base64.encode(resp.getMSS_StatusResp().getMSS_Signature().getBase64Signat
ure()), "ASCII") +"\n\n");
                } catch (UnsupportedEncodingException e) {
                log.info("Unsupported encoding", e);
                }
                try {
                for(PersonIdAttribute a : resp.getPersonIdAttributes()) {
                System.out.println(a.getName() + " " + a.getStringValue());
                }
                } catch (NullPointerException e){
                log.warn("No Person ID Attributes found!");
                }
        }
        ….
```

8.5 Conclusion

The result of this study shows how different mobile certificate based solutions for IT services can be achieved with the assistance of the literature presented in this thesis. The proposed solutions are initiated on Internet, with SMS or during a phone call. During a

phone call, the staff member uses the web interface for providing services to the user. The proposed solutions are limited in the way that there is no access to the Subscriber Identity Module (SIM).

In this thesis, there are still certain things that might be done differently or maybe in a more detailed process and with more consideration of the security that might be required for protection against threats in the future. There are many other ways to design the presented test cases. Therefore the created test cases are probably not the best possible solutions.

The mobile certificate based services (sections 6-7) and the test cases (section 8) can be preliminary guidelines for how mobile certificate based services can be provided by health centres and how these services can be implemented in a health centre's information system.

The collection of proposed mobile certificate based solutions for health centre IT services can be used for providing new ways for a user to authenticate or sign a commitment that a health centre provides. This process not only fastens the process, it is even easier and more reliable for the user to use and also neither users nor staff members need to be present to be able to use some of these services.

The implementation of the proposed mobile certificate based solutions for health centre IT services can be created in different ways. Therefore one possible implementation is described without the technical details of how it is created.

The test cases are examples of how some of the services can be created and therefore deliver users the understanding of how the test cases can be used. The signature of a digest content was left out, since operators do not currently support it.

Future research could use the Interactive Voice Response (IVR) and other communication channels as new methods for providing mobile certificate based services. Furthermore Vetuma can also be used for authentication and payment. Vetuma is a public administration's joint service for citizen authentication and payment (Vetuma, 2011).

Vetuma introduced 20.4.2012 for citizens an additional method for authentication and payment with mobile certificates (Ministry of finance, 2012).

REFERENCES

Espoo. 2012, Self-care [Www]. Available: http://omahoito.espoo.fi/public/espoo-en/Pages/default.aspx Retrieved 1.2.2012.

ETSI. 2003a, TR 102 203 V1.1.1 (2003-05) [Pdf]. Available: http://docbox.etsi.org/EC_Files/EC_Files/tr_102203v010101p.pdf Retrieved 29.3.2012.

ETSI. 2003b, TS 102 204 V1.1.4 (2003-08) [Pdf]. Available: http://docbox.etsi.org/EC_Files/EC_Files/ts_102204v010104p.pdf Retrieved 28.3.2012.

ETSI. 2011, About ETSI [Www]. Available: http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx Retrieved 29.3.2012.

FiCom. 2012a, Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry [Www]. Available: http://www.ficom.fi/lyhyesti/index.html Retrieved 4.2.2012.

FiCom. 2012b, FiCom's (The finnish federation for telecommunications and teleinformatics) application guideline for ETSI's MSS standards: V2.1 [Pdf]. Available: http://www.mobiilivarmenne.fi/linked/fi/MSS_FiCom_Implementation_guideline_2.1.pdf Retrieved 15.2.2012.

KanTa. 2009, National Archive of Health Information [Www]. Available: https://www.kanta.fi/en/national-archive-of-electronic-health-records Retrieved 25.3.2012.

Ministry of finance. 2012, Inloggning till offentliga tjänster med mobil i framtiden [Www]. Available: http://www.vm.fi/vm/sv/03_pressmeddelanden_och_tal/01_pressmeddelanden/20120420Inlogg/name.jsp Retrieved 20.4.2012.

Mobiiliasiointivarmenne. 2011, Varmennepolitiikka Operaattoreiden mobiiliasiointivarmenteita varten: V1.1 [Pdf]. Available: http://www.mobiilivarmenne.fi/linked/fi/Mobiiliasiointivarmenne-Varmennepolitiikka.pdf Retrieved 1.2.2012.

Mobiilivarmenne. 2010, Mobile certification launched in Finland [Www]. Available: http://www.mobiilivarmenne.fi/en/en_7.html Retrieved 2.2.2012.

Mobiilivarmenne. 2011a, Mobile certificate (Mobiilivarmenne) [Www]. Available: http://www.mobiilivarmenne.fi/en/index.html Retrieved 1.2.2012.

Mobiilivarmenne. 2011b, Mobile certificate provides added security [Www]. Available: http://www.mobiilivarmenne.fi/en/en_1.html Retrieved 1.2.2012.

Mobiilivarmenne. 2011c, Frequently Asked Questions [Www]. Available: http://www.mobiilivarmenne.fi/en/en_5.html Retrieved 2.2.2012.

Roger R. Dube. 2008, Hardware-Based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography. ISBN: 978-0-470-1 9339-6.

Sourceforge 2011, Laverca 1.01. [Www]. Available: https://sourceforge.net/projects/laverca/files/1.01/ Retrieved 23.2.2012.

Vetuma. 2011, Citizen identification and payment service Vetuma [Www]. Available: http://www.suomi.fi/suomifi/workspace/shared_services/vetuma/index.html Retrieved 1.4.2012.