**3GPP TSG SA WG3 Security — S3#29 ad hoc** **S3z030018**
**3 – 4 September 2003**
**Antwerp, Belgium**

**Agenda Item:** 5.3

**Source:** Nokia

**Title:** Generic Authentication Architecture and Release 6 services

**Document for:** Discussion

## 1. INTRODUCTION

In S3 # 29 meeting it was decided that to reduce potential security and technical problems and also save costs, a generic authentication architecture (GAA) should be established and used with R6+ new services as much as applicable. In [S3-030407], presented in SA#29 and also attached to this contribution, it was indicated how subscriber certificates could be used with various services. Those include alternative access (section 3.1), Presence (section 4.3.1) and MBMS (section 4.3.7), as well as many other services. It has been proposed in [S3-030256] to use bootstrapping for Presence. GAA model 2 in Nokia's accompanying contribution "Proposal for Generic Authentication Architecture" contains both BSF (for establishing shared key material between UE and the network based on AKA) and PKI portal (for enrolling subscriber certificate based on the shared key).

The new Release 6 services include Presence, WLAN interworking, and MBMS. In this contribution we argue that it is possible to use shared keys bootstrapped from AKA by UE and BSF for those services, except for WLAN access authentication, which is agreed be done using EAP/AKA or EAP/SIM.

In addition, migration to certificate-based solution is possible in later releases.

## 2. DISCUSSION & CONCLUSION

The generic BSF requirements (see chapter 4 of S3-030317) seem to apply for Presence and MBMS.

- The expected requirements for authentication and key agreement in Presence are very similar to those of BSF. For that reason similar interfaces to those of BSF need to be defined if we adopt Presence-specific authentication solution. The only way to avoid specifying and implementing those interfaces is to use IMS-based bootstrapping of shared keys for Presence service but using this solution with other non-IMS services might cause complications. Also, we should avoid the co-existence of several bootstrapping procedures in the 3G architecture as stated by GAA requirement 4 (see S3z030003).

- In case of MBMS, the user authenticates to Broadcast/Multicast Service Center (BM-SC), run by operator or a service provider, to achieve keys with which decryption of multicast content streams etc. is possible. The authentication could utilize shared keys obtained from BSF. Also the expected requirements for authentication and key agreement in MBMS are similar to those of BSF.

- As to the WLAN, in the scenario 3 of WLAN interworking UE establishes a secure communication tunnel to the home operator's network in order to access services provided by UE's home operator. The BSF could be used to establish a shared key material between UE and the home network that is needed to secure the communication tunnel.

In summary, it seems possible to use shared keys bootstrapped from AKA by UE and BSF for the majority of new Release 6 services.

## 3. REFERENCES


S3-030256 “Analysis of HTTP authentication”, S3#28, Nokia.

S3-030317 "Draft TS ab.cde version 0.2.0: Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)", S3#29, Nokia.

S3-030407 “Bootstrapping and subscriber certificate use cases”, S3#29, Nokia.

S3z030003 “Generic Authentication Architecture requirements”, S3 adhoc 2003, Siemens.

**3GPP TSG SA WG3 Security — S3#29** **S3-030407**
**15 –18 July 2003**
**San Francisco, USA**

**Source:** **Nokia**

**Title:** **Bootstrapping and subscriber certificate use cases**

**Document for:** **Discussion**

**Agenda Item:** **7.9, Support for subscriber certificates**

# Contents

## 1. INTRODUCTION

This document describes several use cases for subscriber certificates that are enrolled using AKA and bootstrapping procedure. The bootstrapping procedure and subscriber certificate enrollment based on this procedure are being standardized in 3GPP for Rel6. Subscriber certificate enrollment will use the key material agreed on during bootstrapping procedure for subscriber authentication and for protecting the integrity of exchanged data.

The range of applications and standards that can utilize subscriber certificates or bootstrapping is wide. Cellular network can certify subscriber's cellular identity. Any application that can use cellular identity may benefit from subscriber certificates. Liberty alliance and other standardization forums may have additional certificate usage specifications. But we also note here that there may be other ways to provide security for the use cases included in this document, which are different from what we describe, or that do not use bootstrapping and subscriber certificates.

## 2. GENERAL REQUIREMENTS AND PRINCIPLES

When security of one, bootstrapped, system is initalized from that of another, the bootstrapped system may use longer keys, or better cryptographic algorithms. But, the general security of bootstrapped system depends on the security procedures in the system based on which the bootstrapping is done. This affects the type of applications that can be based on bootstrapping or subscriber certificates. For example, the key length and the format of certificates issued by a bank to its customers may be the same as the key length and the format of certificates issued by PKI-portal Network Application Function (NAF). But certificates issued by a bank may be used in higher-value transactions than certificates issued by a cellular operator because, among other things, a person typically goes through more security checks when she applies for a bank account as compared to when she applies for cellular subscription.

There is a clear advantage in the verifier of digital signature being able to find out at verification time the enrollment procedure of the verifying key. It allows the verifier to abort a transaction if he has concerns over the enrolment procedure's security and it reduces the scope of misunderstandings. A CA may implement this capability by including the description of enrollment procedure in a Certificate Practice Statement (CPS) [RFC2527] and refer to this CPS in the Certificate Policies extension (see section 4.2.1.5 of [RFC3280]) of the certificate itself.

WAP Certificate and CRL Profiles Specification [WAP-cert] is the working assumption for the certificate format in 3GPP.

### 2.1 Common prerequisites

*The common prerequisites* for all use cases presented in this document are:

1. UE has established IP connectivity.

2. User terminal has direct access to USIM.

3. User terminal has requested and received subscriber certificate from the operator's PKI Portal (i.e. NAF), based on cellular subscription and USIM authentication.

4. The fetched certificate is either for authentication, or authorization.

5. The identity carried in the certificate reveals or hides the real user identity depending on the context of certificate usage. Certificate request must indicate the intended context to get the signing for the correct identity and/or attribute certificate. Network needs to implement configuration for the identity mapping.

6. The peer at the other authentication or authorization endpoint knows operator's signature verification key.

7. User terminal is able to verify the certificate of the other (authentication) endpoint (this is enabled e.g. by the terminal fetching the operator CA certificate from the PKI Portal NAF).

## 2.2 Support of TEs

Extending the scope of the subscriber certificates outside the cellular domain to SIMless terminals adds a wide variety of new use cases. Non-cellular terminal support is essential for several alternative access authentication cases where laptop or PC is more convenient terminal than a cellular handset. This section is also relevant for SA3 WI "Feasibility study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces" (S3-030307).

The cellular terminal can support usage of bootstrapping or subscriber certificates in SIMless terminal in many different ways. The following four cases are identified:

1. MT does bootstrapping and certificate request for TE's public key, and then MT gives the received subscriber certificate to TE.

2. PTP type of operation according to MeT specifications, i.e. keys and certificate are stored in MT, and TE request MT to perform needed actions using PTP protocol. [MeT]

3. MT provides bootstrapping interface to TE (keys would stay in MT and TE could request MT to do operations using those keys) and TE does certificate request (or use other NAFs).

4. MT does bootstrapping, then MT gives the shared keys to TE, and TE does certificate request.

Case 1 is illustrated in Figure 1. In flow 1 a public key is transferred from user's laptop to her mobile phone over location-limited (e.g. infrared) channel. The user's key pair may be in a laptop, or in a smart card connected to the laptop's smart card reader. In flow 2 the phone performs bootstrapping procedure with the cellular network and obtains a certificate for user's public key. The user must authorize this operation, for example, by entering a PIN into her phone. In flow 3 the certificate is transferred back to the laptop and installed in laptop's certificate store or into user's smart card. In stage 4 applications use the certified key pair for signing. If operator CA's certificate is also obtained in flow 2 and installed to the laptop, or smart card in flow 3, applications may use it when verifying digital signatures in stage 4. For concreteness, we will assume case 1 in the remainder of this text.

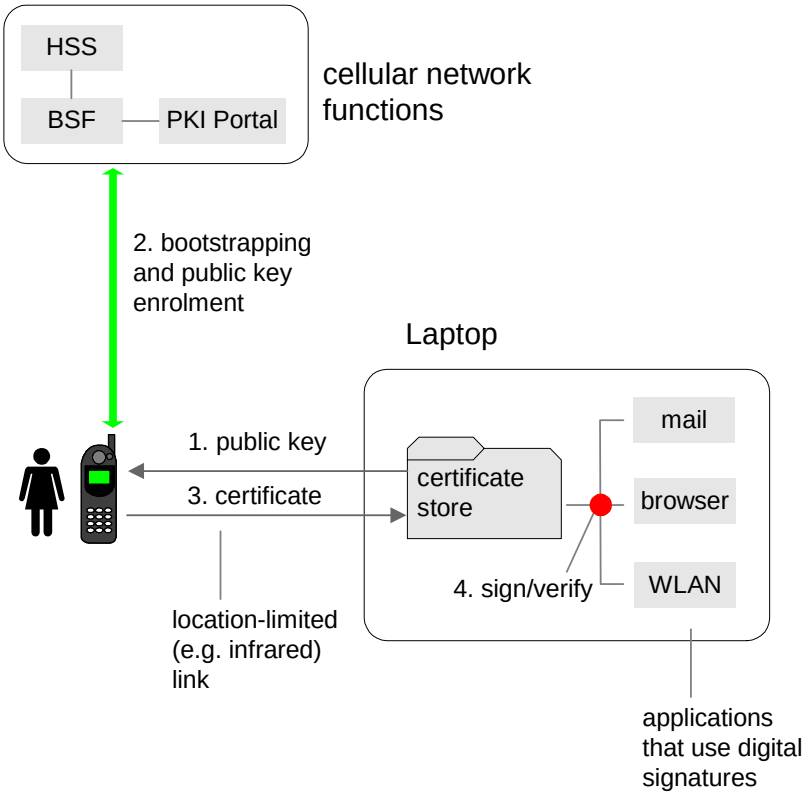


**Figure 1: Illustration of case 1. The public key is transferred from user's laptop to the phone over location-limited link and then certified by the cellular network.**

### 2.3 Linked enrollment

Subscriber certificate may be used in authenticating the UE towards application server, as shown in Figure 2. It may be also used in enrolling another certificate, possibly from a different CA. The UE will use the second certificate in authenticating towards application server. The second enrolment has two main uses: First, it may require security checks in addition to digital signature verification. If the user passes those additional checks, then, for example, she may use services of higher value than with standard certificate. Second, the certificate obtained during the second enrolment may contain non-standard extensions, with application, or vendor-specific attribute values, as shown in Figure 3.

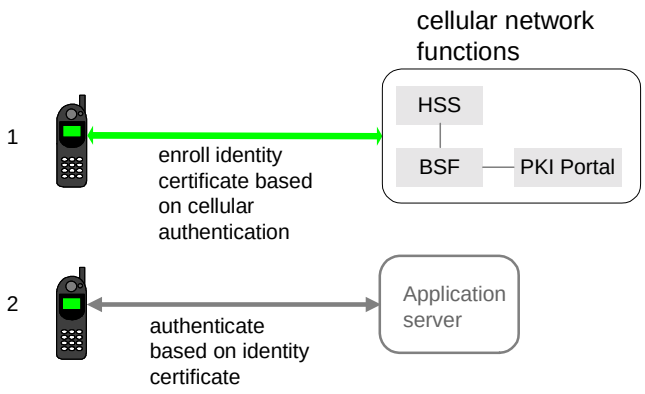


**Figure 2: Using identity certificate obtained from cellular network in authenticating towards application server.**

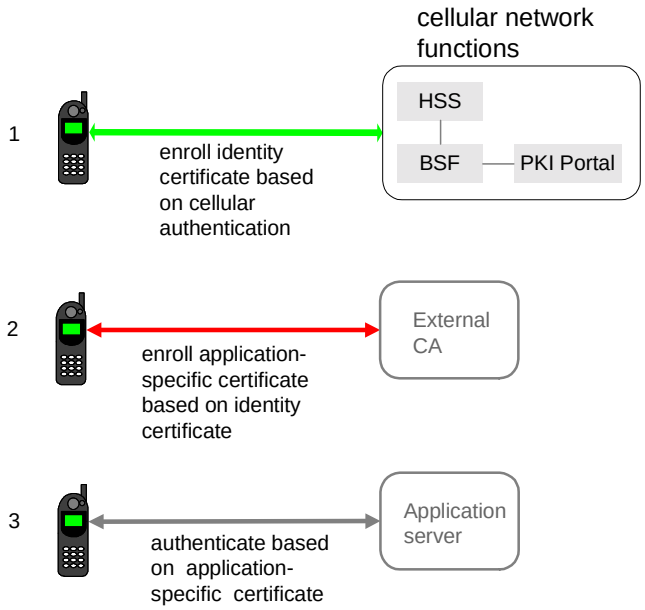


**Figure 3: Using identity certificate obtained from cellular network in enrolling application-specific certificate.**

## 2.4 Giving rights to access private data

It is also possible that cellular user issues *assertions* (e.g. Security Association Markup Language [SAML] assertions) to other users or servers (called viewers below). The assertion could, e.g., allow viewer access to confidential data (e.g. location or presence information) of the cellular subscriber. The cellular subscriber is able to control the granted access rights conditions (e.g. time period) easily because assertions containing those rights are issued from his terminal. The scenario is that the subscriber first authenticates the viewer based on public key of the viewer and then sends an assertion with the viewer's public key and description of the access rights granted to the viewer. The application server storing cellular subscriber's confidential data verifies that the viewer holds the matching secret key when the assertion is presented.

# 3. SECURE CONNECTIVITY

## 3.1 Alternative access authentication

The alternative access cases cover WLAN, DSL and cable modem access to the Internet and other networks.

There are two ways how the subscriber certificates could be used in relation with non-cellular access service. First, subscriber certificates could be used to enable paying for access. Especially in the public access network case, the subscriber and access provider need a mechanism to sign the common understanding of the access cost. The payment could be through phone bill, or some other bill created by cellular operator. For further description of this use case see section 4.4.

The second alternative is that subscriber certificates would be used in access authentication. In the case of separate mobile phone and TE (e.g. laptop), the mobile could deliver the subscriber certificate to the laptop, as illustrated in Figure 1. The benefit of this approach is that there are ready applications for access authentication based on digital signatures and certificates in Windows terminals. TLS Handshake Protocol [RFC2246] provides mutual authentication with server and client certificates. Windows terminals have HTTPS and EAP/TLS clients.

### 3.1.1 Corporate WLAN access authentication

In this scenario corporate WLAN access authentication to corporate subscribers is provided. Corporate subscriber and corporate WLAN access network can mutually authenticate each other. E.g. TLS handshake protocol can be used [RFC2246]. Whether cellular authentication and key agreement (and thus subscriber certificates) are sufficient to access a company's network depends on that company's size and also on what kind of business the company is doing.

**Prerequisites:**

1. Both corporate WLAN manager and the subscriber trust home operator's CA. This is simple to achieve if the corporate has a consistent policy to get all the employer's subscriptions from a single operator.

2. WLAN access controller holds a certificate signed by the home operator's CA. The provider gets the certificate as part of the business agreement with the operator.

3. Subscriber holds a short-term certificate signed by the home operator's CA. The subscriber gets the certificate from the PKI portal.

4. Both WLAN provider and subscriber hold home operator's CA (self signed) certificate to be able to verify the signatures in other certificates.

**User experience:**

The subscriber optionally types the *access PIN* to allow signing with the private key during the access authentication. The purpose of access PIN is to protect from authenticating with a lost or stolen terminal. Exchanging the terminal and access network certificates, validating them and verifying the identity is comparable to HTTPS authentication over DSL or LAN. The delay perceived by the user is not significant. Easy certificate download is essential when WLAN access is terminated in TE.

### 3.1.2 Broadband access

This usage case contains two scenarios:

1) mobile operator owns broadband access network (e.g. DSL or cable modem), or

2) mobile operator provides authentication service to another, broadband access operator.

The subscriber certificate can be issued in the cellular domain and used in broadband access from another terminal (see section 2.2).

**User experience:**

The subscriber optionally types the *access PIN* to allow signing with the private key during the access authentication. The purpose of access PIN is to protect from authenticating with a lost or stolen terminal. Exchanging the terminal and access network certificates, validating them and verifying the identity is comparable to HTTPS authentication over DSL or LAN. The delay perceived by the user is not significant. Easy certificate download is essential in case where WLAN access is terminated in TE.

## 3.2 Service authentication

### 3.2.1 VPN authentication

This user case allows user authentication to VPN gateway, run either by operator or corporate, to achieve secure corporate access. The user can have either mobile or fixed network access (e.g. GPRS, WLAN, xDSL).

During the authentication between the VPN Client and the VPN gateway, subscriber's private key and the subscriber certificate are used in standard fashion (no changes needed in VPN components). It is also possible to issue application-specifc certificate for VPN access based on subscriber certificate as illustrated in Figure 3. The VPN gateway is able to verify the user's signature with the aid of the certificate it received from the user during the authentication protocol. The end result is that user has established a secure end-to-end tunnel from the terminal to the VPN gateway.

**Prerequisites:**

The common prerequisites as described in section 2.1. The certificate is for *authentication*. The VPN gateway knows operator's signature verification key. In the case of a single enterprise running several VPN gateways there will be an intermediate enterprise CA that authorizes the authenticated users. The functionality of VPN gateways is simplified if the enterprise CA checks the mapping between cellular and enterprise identities before issuing VPN certificate. In this case the VPN gateways need to verify only UE signature and its VPN certificate.

**User experience:**

The subscriber optionally types the *access PIN* to allow signing with the private key during the VPN client authentication. The purpose of access PIN is to protect from authenticating with a lost or stolen terminal. Exchanging the terminal and access network certificates and verifying the identity is part of standard IKE authentication. Cellular wireless connection (GPRS or WCDMA) may cause significant delay for the user.

The VPN client should automatically select the correct identity and certificate to be sent to the VPN gateway to improve usability. For maximum flexibility, the VPN client should be able to ask the user which identity to use.

# 4. SECURE SERVICES

## 4.1 Person-to-person

### 4.1.1 Peer-to-peer authentication

The subscriber certificates can be used in various cases where peer-to-peer authentication is needed. Possible application are e.g. file transfer, printing, adhoc networking.

One example scenario is that two subscribers authenticate each other in order to, e.g. exchange authenticated e-mail messages. The recipient can be sure that the messages came from the purported sender, if she knows sender's phone number. The certificate used is an identity certificate – it is a normal subscriber certificate that includes subscriber's phone number. This scenario can be used with several applications, e.g. MMS, S/MIME, or chatting. It is important to note that the peer-to-to-peer authentication can be applied in an adhoc local environment, e.g. over Bluetooth.

**Prerequisites:**

The common prerequisites as described in section 2.1. Additionally both parties need to be able to verify each other's subscriber certificates (i.e. to have subscriber certificates from same operator, or have corresponding operator CA certificate).

**User experience:**

The peer-to-peer authentication consists of authenticating oneself towards the peer and verifying peer's identity.

- During authentication subscriber types the access PIN to allow access to the corresponding signing key. The purpose of access PIN is to protect from authenticating with a lost or stolen terminal. (If the signature is meant for non-repudiation purposes, then the data being signed should be also shown to the subscriber by a trusted application in the terminal.)

- During verification of peer's signature, subscriber needs to be notified, e.g. visually, about the owner of the received certificate. If this is the first encounter with the peer, then, e.g., the subject field of the peer's certificate will be shown and the subscriber will be asked whether she wants to trust that certificate. If this is not the first encounter with the peer, and peer's certificate has been previously imported to subscriber's terminal, then only a pseudonym for the certificate assigned by subscriber may be shown.

## 4.2 Corporate services

### 4.2.1 Authentication to corporate intranet applications

In this scenario, the subscriber certificate is used to authenticate the user towards corporate's intranet applications (e.g., e-mail service). Whether cellular authentication and key agreement (and thus subscriber certificates) are sufficient to access a company's network depends on that company's size and also on what kind of business the company is doing.

**Prerequisites:**

1. User's certificate and the corresponding private key are present in the Windows certificate store (or alike). This may be achieved as shown on Figure 1

2. User has access to corporate network.

3. Corporate applications are able to use user certificates for authentication.

**User experience:**

The usage of certificate-based authentication towards corporate applications can be done in two ways:

1. single logon to the corporate network where the user certificate (and the corresponding private key) are used for authentication during either logon to the Windows domain (i.e., direct connection to corporate's intranet is available), or initialization of a VPN connection as described in section 3.2.1.

2. case by case logon where the user certificate is manually selected by the user during the application specific authentication step. It may be that that some intranet applications require additional authentication, possibly with a different key pair.

In both cases, a passphrase is asked to unlock the private key usage in the certificate store. In single logon, the passphrase could be cached and subsequent authentications done automatically. Of course, it should also be possible to ask the passphrase each time a digital signature is required. This could be a configurable feature, e.g., ask the passphrase: a) once, b) once per application, or c) always.

The actual authentication steps depend on corporate intranet application (e.g., TLS for web based access to Outlook).

## 4.3 Person-to-content

### 4.3.1 Access to Presence services

User authenticates to operator's authentication proxy, to achieve secure access for Presence services. The user can have either mobile or fixed network access (e.g. GPRS, WLAN, or xDSL). The authentication could utilize either shared keys obtained from bootstrapping or subscriber certificate. E.g. the UE could use subscriber certificate in TLS authentication with authentication proxy. The benefit of using certificates is that off-the-shelf TLS gateway can do the authentication in authentication proxy.

**Prerequisites:**

The common prerequisites as described in section 2.1.

**User experience:**

The authorization solutions may be based directly on subscriber certificates, or they may be based on a combination of authentication with subscriber certificate and access control list in the Presence server. In the first case the viewer may remain anonymous towards the Presence server (see section 2.4) The server

- receives an assertion signed by the data owner, which contains a public key and set of access rights,
- verifies that the viewer (sender of the assertion) holds the matching private key and
- allows secure access (e.g. TLS connection) only if the verification succeeds.

### 4.3.2 Self-service management

This scenario allows user to authenticate to a Web portal, run by operator, to achieve secure access for self-provisioning. Secure end-to-end (TLS) tunnel from the terminal to the Web portal can be established (subscriber's private key and the certificate are used in

standard fashion, i.e. no changes needed in TLS components). The user can have either mobile or fixed network access (e.g. GPRS, WLAN, or xDSL). The main use cases are billing information queries and modifying one's subscription profile.

**Prerequisites:**

The common prerequisites as described in section 2.1.

**User experience:**

The authorization may be based directly on subscriber certificates, or on a combination of authentication with subscriber certificate and access control list in the Web portal. In the first case the self-management server:

- receives an assertion signed by the data owner, which contains a public key and set of access rights,
- verifies that the sender of the assertion holds the matching private key and
- allows the secure access (e.g. TLS connection) only if the verification succeeds.

4.3.3 Secure access to operator's Web services

The operator provides the content service and relies on the two-way HTTPS authentication based on subscriber certificate. Subscriber could use operator's portal to access cellular network services (e.g. to store and send SMS/MMS), or to access operator's Web services (e.g. ringing tones, logos, picture messages, chat and dating, astrology, games and entertainment, traffic and automobiles, news and weather, business news, sports and gambling).

**Prerequisites:**

The common prerequisites as described in section 2.1.

**User experience:**

The subscriber optionally types the *access PIN* to allow signing with the private key during the access authentication. The purpose of access PIN is to protect from authenticating with a lost or stolen terminal. Exchanging the terminal and access network certificates, validating them and verifying the identity is comparable to HTTPS authentication. The perceived QoS depends on access network delay.

4.3.4 Secure access to 3rd party content services

In this scenario a 3rd party provides the content service and relies e.g. on the two-way http/tls authentication or assertions (see section 2.4). The provider needs a service level agreement with the cellular network operator. The prerequisites and user experience are as in section 4.3.3.

One example of this use case is location service portal where authorized friends can query the subscriber's location. In this case strong authorization may be needed to protect user's privacy. Another example is user's photo album in 3rd party's server that is accessible to her friends.

4.3.5 Enhanced LCS privacy

In this scenario subscriber certificates are used to enhance the LCS codeword security in two ways. First, only the intended LCS client or requestor can use the codeword. Second, the subscriber remains anonymous towards LCS client and requestor.

The target UE (user) may issue and sign an enhanced codeword, which gives permission to particular LCS client or requestor to access user's location information. The enhanced codeword contains: enhanced codeword identity, optionally requestor identity, LCS client identity, validity period, number of usage times, Home-GMLC address and possibly other parameters. UE delivers this enhanced codeword and home operator issued subscriber certificate or subscriber certificate URL to the LCS client or requestor.

The LCS client can use the enhanced codeword for UE location query in the following way: The LCS client sends location request with the enhanced codeword to R-GMLC (Requesting GMLC), which forwards it to Home-GMLC. Only the H-GMLC shall check whether the enhanced codeword received from the LCS client is acceptable, with the help of the corresponding subscriber certificate. If codeword is accepted the H-GMLC locates the user, and delivers location information back to R-GMLC, which forwards it to LCS Client.

**Prerequisites:**

The common prerequisites as described in section 2.1.

**User experience:**

UE user verifies LCS client identity and chooses if he wants to reveal his location. If he does, the UE signs the enhanced codeword with the private key for the permission. The LCS client SW forwards the codeword automatically to the R-GMLC. There is not necessarily a human user in LCS client endpoint at all. In case there is, he will be unaware of the codeword usage and the technology underneath. The location information target UE can be sure that only the intended LCS client can use the enhanced codeword. The target UE remains also anonymous toward LCS client and requestor.

#### 4.3.6 Notifications through cellular network

In this scenario subscriber authorizes the operation of sending notifications by service provider through the cellular network. The service provider does not need to know subscriber’s identity. If there is no identity information in the certificate, then the subscriber may remain anonymous towards the service provider. However, subscriber may pay for the notifications through his phone bill. Subscriber authorizes such payment and the charging is triggered when the service provider sends a notification.

**Prerequisites:**

The common prerequisites as described in section 2.1.

**User experience:**

During a transaction UE sends to the service provider an assertion, i.e. signed authorization, to send a notification message to that UE through the cellular network, and subscriber certificate or subscriber certificate URL. The service provider verifies the authorization text and UE’s signature with the aid of subscriber certificate. If the signature and the authorization text are correct, then the service provider will send a positive acknowledgement to the UE.

At a later time, for example when a certain sport’s event takes place, the service provider creates a notification and submits it to the operator together with the signed UE’s authorization and subscriber’s certificate. The operator verifies the signed authorization. If the verification succeeds the operator will forward the notification text to the subscriber in an SMS or MMS message.

#### 4.3.7 MBMS security

In this scenario the user authenticates to Broadcast/Multicast Service Center (BM-SC), run by operator or a service provider, to achieve keys with which decryption of multicast content streams etc. is possible. The authentication could utilize either shared keys obtained from bootstrapping or subscriber certificate. The user can have either mobile (3GPP Release6 case) or fixed network access (e.g. GPRS, WLAN, or xDSL).

**Prerequisites:**

The common prerequisites as described in section 2.1.

**User experience:**

The user connects to BM-SC and e.g. TLS authentication takes place. During the authentication between the user's Web client and the Web server (in BM-SC), subscriber's private key and the certificate are used in standard fashion (no changes needed in TLS components). The Web server (in BM-SC) is able to verify the user's signature with the aid of the subscriber certificate it received from the user during the authentication protocol.

#### 4.3.8 Liberty Alliance use cases

Liberty Alliance is an industry consortium that aims to 1) create specifications allowing organizations to build products and services that will interoperate and 2) promote secure federated identity management. [Liberty]

There are two scenarios where AKA bootstrapping or subscriber certificates can be used to augment the infrastructure specified by Liberty Alliance. The first scenario is the authentication of a user agent (UA) to an identity provider (IdP) operated by a cellular operator. This approach leverages the strong, hardware-token based, authentication mechanisms of cellular networks for Liberty. This approach would also increase the scalability of Liberty because a cellular subscriber could potentially use the IdPs of any operator with whom his home operator has a roaming agreement.

A second scenario is to use subscriber certificates in conjunction with terminal-resident discovery service. Terminal-resident discovery service is sensible because it allows the user to exercise policy control over the information related to her identity and profiles. This is done by the discovery certificate issuing credentials to web service clients who need to access identity services related to a user. Subscriber certificates can be used by a web service provider to validate such credentials issued by a terminal-resident discovery service to a web service client. This may require a small addition to the Liberty DiscoveryUpdate procedure specification.

These Liberty use cases are described in more detail in following subsections.

##### 4.3.8.1 Authentication of client to identity provider

The Liberty specifications do not specify how exactly client authentication to IdP is to be carried out. However, they do specify various supported "Authentication Contexts" to be used. For example, one authentication context is "MobileDigitalID" which appears to be intended to describe authentication of mobile users based on strong authentication (digital signatures, or TLS/WTLS client authentication). Thus the authentication to IdP could be carried out either by using AKA bootstrapping directly, or by using subscriber certificates.

The use of bootstrapping for IdP authentication could happens as follows. In this case the Liberty IdP acts as a NAF.

1. When the IdP wants to authenticate UA, it sends message to UA indicating that UA-IdP authentication is requested.

2. At this point, UA needs to know that authentication based on AKA bootstrapping is supported by the IdP. UA then initiates the AKA bootstrapping process. After the bootstrapping has been performed, the UA and BSF have a new security association.

3. UA can now send an authentication response to the IdP. This response will be secured using the security association set up in the previous step.

4. In order to verify the authentication response, IdP needs to get the security association from BSF.

Authentication to IdP using subscriber certificates can be done in the following way. In this case, the IdP has no role in AKA bootstrapping. The PKI Portal acts as a NAF.

1. As before, IdP sends message to UA indicating that UA-IdP authentication is requested.

2. At this point, UA needs to know that authentication based on client certificates is supported. If the UA does not have a valid client certificate, it initiates the AKA bootstrapping process. At the end of this step, UA and BSF have a new security association. UA then engages in the subscriber certificate request procedure.

3. At the end of these steps, UA has a valid client certificate, which can be used to prove its authenticity to IdP.

#### 4.3.8.2 Support of terminal-resident discovery service

Liberty web services framework also contains a discovery service (DS) [DS]. Liberty specifications do not mandate where the discovery service is to be located. Since the local access control decision is subject to the discretion and policies of the end user, a natural location for the discovery service is the user terminal. Liberty specifications do already support the possibility of locating some web services on the terminal [PAOS].

It should be possible for a web service provider to verify credentials issued by terminal-resident discovery service. This verification must not require interaction with the terminal. Therefore, these credentials should be in the form of public key digital signatures.

One possibility is to use subscriber certificates. This would work as follows:

1. Web Service Provider (WSP) has a trust relationship with a cellular operator and can verify assertions and certificates issued by this operator’s servers.

2. WSP knows the user by a fixed identity UA-WSP-Id. This is in the access control information associated with that user’s service instances. This access control information is set up when the service instance is created.

3. Terminal-resident discovery service gets a subscriber certificate for UA-WSP-Id for a public key PK

4. To authorize a Web Service Client (WSC), terminal-resident discovery service creates an assertion using the corresponding private key, SK. The credential in the DiscoveryLookupResponse consists of this assertion and the subscriber certificate. The credential may be further encrypted by the WSP’s public encryption key (so that the WSC does not learn the details in the subscriber certificate).

5. Provider access control check then consists of checking that

    i. the subscriber certificate corresponds to identity UA-WSP-Id of the requested service instance

ii. verifying the subscriber certificate

iii. verifying the assertion using PK

As mentioned, Step 2 is done at the time the service instance is created. Suppose we let UA-WSP-Id to be the Liberty pseudonym by which the user is known to WSP. The advantage of this approach is that the access control information is implied and no special access control set up procedure is needed. The disadvantage in this case is that the Liberty IdP and the CA/RA must be tightly coupled so that the CA can check that the sender of a subscriber certificate enrollment request is the owner of UA-WSP-Id.

A second approach is to can let the UA choose UA-WSP-Id to be something other than a Liberty pseudonym. In this case, this information should be conveyed to the WSP. The Liberty discovery service specification contains an update procedure that a WSP can use to update its resource offering advertised by the discovery service [DS]. The response message of this procedure, DiscoveryUpdateResponse, needs an additional (i.e., not in the current specification) optional parameter to convey the access control information from a terminal-resident discovery service. AccessControlInfo is the identity UA-WSP-Id. Since this must be an unspoofable identity, it is either the cellular identity of the subscriber (e.g., MSISDN) or something derived deterministically from it.

### 4.4 Small to medium payment through cellular operator

In this scenario the subscriber authorizes payment for a service through his phone bill (or with separate bill). Note that the provider of the service does not need to know subscriber's identity. If there is no identity information in the certificate, then the subscriber may remain anonymous towards the service provider. The service may be e.g. non-cellular access in an environment where the operator's traditional billing mechanisms are not directly applicable, e.g. non-cellular access is provided by third party (see also section 3.1).

During a payment transaction UE sends to the service provider a signed invoice and subscriber certificate (or subscriber certificate URL). The service provider verifies the UE's signature with the aid of subscriber certificate. If the signature and the invoice are correct, then the service provider will grant UE access to, or deliver the requested service.

In the settlement phase the service provider forwards the signed invoice to the operator for verification. If the verification is successful then the operator will reimburse service provider and charge the subscriber the price of the service through his phone bill (or with separate bill).

**Prerequisites:**

The service provider has a business relationship with operator that issued subscriber's certificate and it knows operator's signature verification key.

If the service provider (e.g. visited access network provider abroad) does not have a direct relationship with the subscriber's home network, the certificate should come from the visited network. The independent access network provider trusts the visited operator as well as the subscriber authentication and certificate from that operator.

**User experience:**

The subscriber trusts the billing from the home operator and payment is convenient. During the service usage he will have to type in the payment PIN for configured amounts. The terminal may automatically sign very small amounts. In this case only larger amounts and cumulative sum above a threshold trigger the PIN query.

## 5. SUMMARY

This document has described various use cases for subscriber certificates and bootstrapping. These use cases can be divided to two main classes: secure connectivity and secure services.

Secure connectivity utilizes cellular infrastructure and existing operators customer relationships to authenticate users. The identified use cases are:

- Alternative access authentication
  - Corporate WLAN access authentication
  - Broadband access, e.g. DSL or cable access
- VPN authentication

Secure services use cases provide convenient and secure way of authenticating cellular subscribers to various services. These services can be provided by cellular operators, corporations, or 3rd party content providers. Secure services may also support billing. The use cases identified in this document are:

- Person-to-person authentication, i.e. peer-to-peer authentication
- Corporate applications, e.g. authentication to corporate intranet applications
- Person-to-content
  - Access to Presence services
  - Self-service management
  - Access to operator's Web services
  - Access to 3rd party content services
  - Enhanced LCS privacy
  - Notifications through cellular network
  - MBMS security
  - Support of Liberty Alliance use cases
- Small to medium payment through cellular operator

All of the mentioned use cases are possible to support with subscriber certificates, many of them are also possible to support with bootstrapped shared keys. This would require that application server implements NAF to obtain shared keys from BSF as illustrated in section 4.3.8.1.

Subscriber certificates offer end users a convenient user experience. Same PIN, that protects access to private key, can be used in authentication to many different services and authorize payments for different service providers.

## 6. REFERENCES

[WAP-cert] WAP Certificate and CRL Profiles, WAP-211-WAPCert, 22-May-2001, http://www.wapforum.org/.

[RFC2246] RFC 2246, The TLS Protocol Version 1.0, January 1999, http://www.ietf.org/rfc/rfc2246.txt.

[RFC2527] RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999, http://www.ietf.org/rfc/rfc2527.txt

[RFC3280] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002, http://www.ietf.org/rfc/rfc3280.txt

[MeT] MeT Personal Transaction Protocol 1.0, November 2002 http://www.mobiletransaction.org/pdf/R200/specifications/MeT_PTP_v100.pdf

[SAML] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML), OASIS standard, 5 November 2002.

[Liberty] Liberty Alliance web page, http://www.projectliberty.org/.

[PAOS] Liberty Reverse HTTP Binding 1.0, Draft version 1.0-08

[DS] Liberty Discovery Service Specification, Draft version 1.0-06