ETSI TS 133 221 V13.0.0 (2016-01)

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Generic Authentication Architecture (GAA);
Support for subscriber certificates
(3GPP TS 33.221 version 13.0.0 Release 13)

Reference
RTS/TSGS-0333221vd00

Keywords
GSM,LTE,SECURITY,UMTS

ETSI

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

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

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

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document describes subscriber certificate distribution by means of generic bootstrapping architecture (GBA) TS 33.220 [11]. Subscriber certificates support services whose provision the mobile operator assists, as well as services that are offered by the mobile operator.

The scope of this specification presents signalling procedures for support of issuing certificates to subscribers and the standard format of certificates and digital signatures. It is not intended to duplicate existing standards being developed by other groups on these topics, and will reference these where appropriate.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] IETF RFC 2986 : " PKCS#10 Certification Request Syntax Standard" Version 1.7 (2000).

[2] IETF RFC 2510: "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

[3] IETF RFC 2511: "Internet X.509 Certificate Request Message Format".

[4] IETF RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[5] Void.

[6] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[7] OMA Security: "Certificate and CRL Profiles", version 1.1 (2004).

[8] OMA Security: "Wireless Identity Module; Part: Security, version 1.2 (2005).

[9] OMA Security: "Wireless Application Profile; Public Key Infrastructure Definition", version 1.2 (2005).

[10] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997: "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework".

[11] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[12] Void

[13] Void.

[14] OMA: "Crypto Object for the ECMAScript Mobile Profile", version 1.1 (2005).

[15] IETF RFC 3546: "Transport Layer Security (TLS) Extensions".

[16] Void.

[17] IETF RFC 3039: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

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

[19] OMA: "Provisioning Content Version 1.1" (2005).

[20] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[21] Void

[22] IETF RFC 2797: "Certificate Management Messages over CMS".

3 Definitions and abbreviations

3.1 Definitions

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

Subscriber certificate: a certificate issued to a subscriber. It contains the subscriber's own public key and possibly other information such as the subscriber's identity in some form.

CA certificate: A Certificate Authority signs all certificates that it issues with its private key. The corresponding Certificate Authority public key is itself contained within a certificate, called a CA Certificate.

3.2 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
B-TID	Bootstrapping Transaction Identifier
blob	Binary Large Object
BSF	Bootstrapping Server Function
CA	Certificate Authority
CMC	Certificate Management Messages over CMS
CMP	Certificate Management Protocols
CMS	Cryptographic Message Syntax
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
MNO	Mobile Network Operator
NAF	Network Application Function
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
UE	User Equipment

4 Support for Subscriber Certificates

4.1 Introduction

Digital signatures can be used, for instance, to secure mobile commerce, service authorization and accounting. But digital signature by itself is not enough; there is need of a global support for authorization and charging. This TS specifies a global and secure authorization and charging infrastructure of mobile networks to support a local architecture for digital signatures.

Subscriber certificates, issued using the mechanisms described in this TS, provide a migration path towards global Public Key Infrastructure (PKI). A local architecture for digital signatures can be deployed incrementally; one operator can choose to deploy independently of the others. On the other hand, the existence of subscribers and service providers that use digital signatures makes it easier to build a global PKI.

3GPP systems shall issue subscriber certificates in order to authorize and account for service usage both in home and in visited networks. This requires specification of:

1. procedures to issue temporary or long-term certificates to subscribers;
2. standard format of certificates and digital signatures, e.g. re-using OMA wireless PKI specifications.

The mechanism shall allow a cost efficient implementation of the security support of the UE. It will also enable a user's anonymity towards the service provider, whilst the user who invokes the service, can be identified by the network.

Open Mobile Alliance offers an alternative solution for certificate enrolment (c.f. subclause 4.5)

Subscriber certificates support services whose provision the mobile operator assists, as well as services that the mobile operator provides. There is no need to standardize those services in this TS. Also, the communication between service provider and the operator (in the role of certificate issuer) need not be standardized in this TS.

4.2 Reference model

Figure 1 shows a simple network model of the entities involved in the certificate issuing, and the reference points used between the network entities.

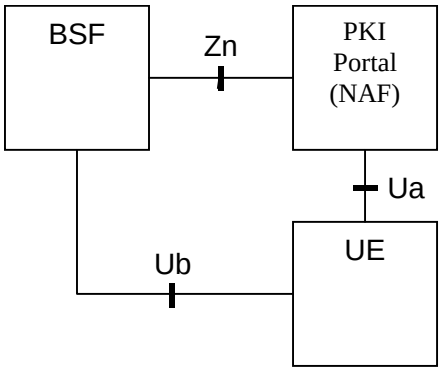

Figure 1: Simple network model for certificate issuing

4.3 Network elements

4.3.1 PKI Portal

A PKI Portal shall issue a certificate for UE and deliver an operator CA certificate. In both cases, requests and responses are protected by shared key material that has been previously established between UE and a BSF.

In PKI terms, the PKI portal is a Registration Authority (RA) who authenticates the certification request based on cellular subscription. PKI Portal may also function as a Certification Authority (CA) who issues certificates. However, this task may also be done in an existing PKI infrastructure towards which the PKI Portal would function as a RA only, and the CA would be in the PKI infrastructure.

4.3.2 Bootstrapping Server Function

The bootstrapping server function (BSF) shall support the PKI portal by providing the authentication and the PKI portal specific user security settings (i.e. whether subscriber is able to enrol a certain types of subscriber certificate).

4.3.3 User Equipment

The required new functionality from UE is the support of the reference point Ua (i.e. certification enrolment protocol) that is protected using the shared keys established during bootstrapping function.

In addition UE may have the capability to generate public and private key pairs, store the private key part to a non-volatile memory (e.g. in UICC), and protect the usage of the private key part (e.g. with a PIN).

4.4 Requirements and principles for issuing subscriber certificates

The following prerequisites for issuing of subscriber certificates exist:

- the UE and the mobile operator's PKI portal share key material to support the certificate request and operator CA certificate retrieval;
- the issuing of the requested certificate is allowed according to subscriber's PKI portal specific user security setting. The PKI portal is responsible for performing this check before issuing the subscriber certificate;
- in the case that the private key is stored on a WIM [8], which is capable of providing a proof of key origin (assurance info that the key is securely stored in a tamper-resistant device), it shall be possible to send this information with the certificate request.

NOTE: Procedures for providing proof of key origin are not limited to the WIM application.

4.4.1 Usage of Bootstrapping

Issuing procedures of the subscriber certificate and operator CA certificate shall be secured by using shared keys obtained from the 3GPP generic bootstrapping architecture as specified in TS 33.220 [11].

4.4.2 Access independence

Subscriber certificate and operator CA certificate issuing procedures are access independent. Certificate issuing procedures require IP connectivity from the UE.

4.4.3 Roaming and service network support

The roaming subscriber shall be able to request subscriber certificates and operator CA certificates from the home network.

The roaming subscriber shall be able to request subscriber certificates and operator CA certificates from the visited network. The home network shall be able to control whether the visited network is allowed to issue subscriber certificates to its roaming subscribers (see clause 4.4.4).

4.4.4 Home operator control

Home operator shall be able to control the issuing of subscriber certificates. The control includes to whom the certificates are allowed to issue and the types of issued certificates.

Operator control is supported by information in the GBA user security settings. For each type of subscriber certificate, i.e. for different key usage in WAP Certificate and CRL Profile [7], subscriber's PKI portal specific user security setting shall contain a flag that allows or disallows the issuing of that type of certificate to subscriber. According to WAP Certificate and CRL Profile [7], there are two types of certificates for users (i.e. subscribers): user certificates for authentication and user certificates for digital signatures (i.e. non-repudiation).

Delivery of operator CA certificates is always allowed.

4.4.5 Charging principles

The operator shall be capable to charge issuing of subscriber certificates or delivery of operator CA certificates.

4.4.6 Subscriber Certificate Profile

Subscriber certificate profile shall be based on WAP Certificate and CRL Profile [7], which in turn is based on profiles defined in IETF RFC 3280 [6] and ITU-T X.509 [10] with the exception that the SHA-1 and SHA-256 hash functions shall be mandatory to support. For security reasons, the use of SHA-1 is not recommended for newly created certificates and CRLs.

NOTE 1: For interworking with pre-Release 9 elements, usage of SHA-1 in certificates and CRLs may be required for some time. However, it is likely that in a future 3GPP release, certificates and CRLs which use SHA-1 as the hash algorithm will be prohibited.

A certificate profile defines the format and semantics of certificates in a specific context. WAP Certificate and CRL profiles specification defines four certificate profiles: two user certificate profiles – one for authentication and the other for non-repudiation purposes, server certificate profile for authentication, and authorization certificate profile (i.e., CA certificate). Since subscriber certificates are issued to users, and since services need CA certificate to validate subscriber certificates, the relevant WAP certificate profiles to be used with subscriber certificate profiles are the user certificate profiles, and CA certificate profile.

Qualified certificate profiles by IETF [17] and ETSI [18] may also be used as the subscriber certificate profile if the certification practices followed by the certificate issuing operator fulfil all of the requirements stated in [16,17,18].

The following certificate extensions may be filled with the information given by the UE in the certification request:

- Intended certificate usage (i.e. using keyUsage and/or extKeyUsage extensions [7]).
- Subscriber identities (i.e., subject name field, and possible additional identities defined in the subjectAltName extension [7]). Operator CA shall authorize each suggested subscriber identity.
- Proof of key origin (i.e., keyGenAssertion). Operator CA shall verify the proof of key origin if it is presented.

NOTE 2: It is not mandatory for Operator CA to insert these suggested extensions by UE to the certificate. Rather, Operator CA shall issue certificates based on its certification policies. It may write a certification practice statement (CPS) [4], where it describes the general requirements and steps taken during the certificate issuing.

4.4.7 Service Discovery

To enable the certificate enrollment procedure, the addresses of bootstrapping server and PKI portal should be configured to the UE. The BSF discovery method is specified in TS 33.220 [11].

A procedure needs to be described on how to discover the location of PKI portal. It shall be possible to enable the UE to be configured either manually or automatically via one of the following approaches:

- The address information shall be published via reliable channel. Subscribers shall store all the parameters as part of the establishment of IP connectivity. The address information needs to be input only once.
- The address information shall be pushed automatically to the UE over the air when the subscription to bootstrapping service is accepted. All the parameters shall be saved into the UE and used in the same manner as above. The procedure is specified in OMA's "Provisioning Content Version 1.1" [19].

4.4.8 Requirements on reference point Ua

The requirements for reference point Ua are:

- UE shall be able to request for subscriber's certification from the PKI portal that plays the role of the NAF over a network connection;
- NAF shall be able to authenticate UE's certificate request;
- UE shall be able to acquire an operator's CA certificate over the network connection;
- UE shall be able to authenticate the NAF response (i.e., operator CA certificate delivery);
- the procedure shall be independent of the access network used;
- the NAF shall have access to the subscriber's PKI portal specific user security setting to check the certification policies. This means that the reference point Zn TS 33.220 [11] shall support for retrieving a subset of the GBA user security settings;
- the response and delivery of certificate to UE shall be within a few seconds after the initial certification request;
- certification request format shall be PKCS#10;
- certification response format shall be one of the following: a certificate, a pointer to the certificate, or a full certificate chain.

4.5 Certificate issuing architecture

4.5.1 Reference point Ua

4.5.1.1 General description

In the certificate issuing, reference point Ua is used to for:

- The operator CA certifying subscriber's public keys in format of certificates; and
- The delivery of the Operator CA certificate to the UE.

During subscriber certificate issuing, UE may request a certification of a public key. The supported request format shall be PKCS#10. It is used to encapsulate the public key and other attributes (i.e., subject name, intended key usage, etc.). The request is transported from the UE to the PKI Portal over reference point Ua. Upon receiving the certification request, the PKI portal will certify the public key according to its own certification practice policies and subscriber's PKI portal specific user security setting which is fetched through BSF from HSS. If PKI Portal decides to certify the public key, it will digitally sign it, and generate the corresponding certificate, which is returned from PKI Portal to the UE, over reference point Ua.

During operator CA certificate delivery, the UE may request the PKI Portal to deliver operator CA's certificate. In the corresponding response, the PKI Portal will deliver the CA's certificate to the UE. Since the operator's CA certificate is typically a self-signed certificate and the validation of certificates signed by this CA is based on this particular CA certificate, it needs to be delivered over authenticated and secured channel.

Authentication, integrity protection, and possibly encryption of the messages sent over reference point Ua are based on the BSF generated shared secret according to the GBA in TS 33.220 [11], where the PKI portal acts as a Network Application Function (NAF).

4.5.1.2 Functionality and protocols

4.5.1.2.1 PKCS#10 with HTTP Digest Authentication

A PKCS#10 [1] based certification request is sent to the PKI portal using a HTTP request, which shall be authenticated and integrity protected by HTTP Digest Authentication as specified in clause 5.2 of TS 24.109 [20].

Certificate is delivered using the HTTP response, which may be authenticated and integrity protected by HTTP Digest Authentication. The content-type of the HTTP response depends on the response format. If a certificate is returned then it is "application/x-x509-user-cert". If a pointer to the certificate is returned then it is "application/vnd.wap.cert-response" as specified in WPKI [9]. If a certificate chain is returned, then it is "application/pkix-pkipath" as specified in IETF RFC 3546 [15].

The UE requests a CA certificate delivery by sending a plain HTTP GET request with specific parameters in the request URI. The request may be authenticated and integrity protected by HTTP Digest Authentication.

CA certificate is delivered using the HTTP response, which shall be authenticated and integrity protected by HTTP Digest Authentication. The content-type of the HTTP response would be "application/x-x509-ca-cert". Note that the user should always be notified when a new CA certificate is taken into use.

4.5.1.2.2 Key Generation

If the private key is stored in a UICC (e.g. in a WIM [8]) and the UICC demands a special authorization (e.g. from the Operator) to generate the key, the ME may need to perform an HTTP request, which may be authenticated and integrity protected by HTTP Digest Authentication, to the NAF in order to deliver a nonce that is generated by the UICC. This will allow the NAF to authenticate directly to the UICC application and provide authorization for the key generation. The exact key generation procedure is specified in OMA's "Crypto Object for the ECMAScript Mobile Profile" [14].

4.6 Certificate issuing procedure

4.6.1 Certificate issuing

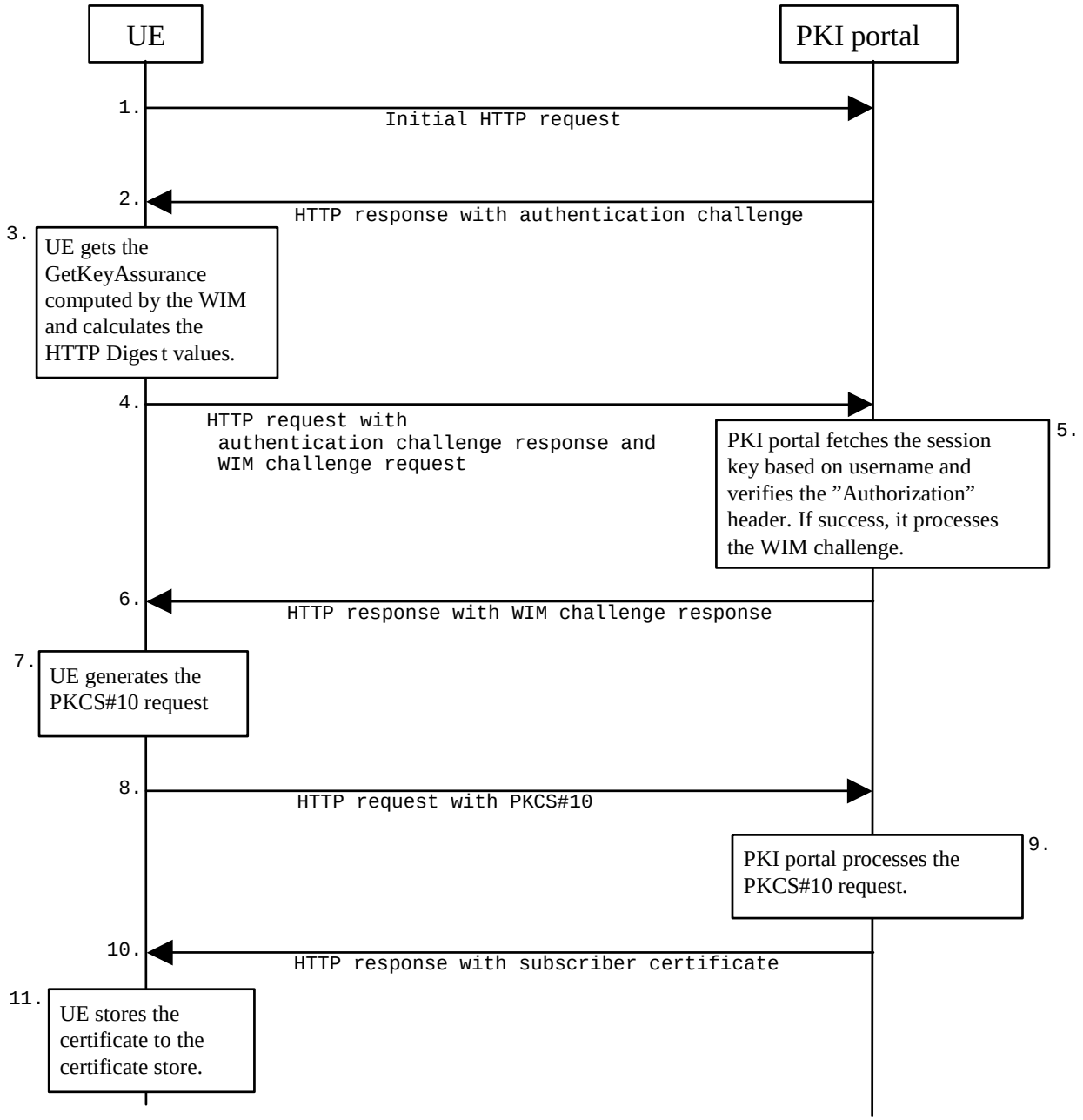

Figure 2: Certificate request using PKCS#10 with HTTP Digest Authentication

The sequence diagram above describes the certificate request when using PKCS#10 with HTTP Digest authentication. The actions involving WIM application in steps 3-6 shall be omitted if there is no WIM application in the UE. The procedure is secured as specified in clause 5.2 of TS 24.109 [20]. The detailed definition of the messages is left to stage 3 specifications.

1. The sequence starts with the UE sending an empty HTTP request to the PKI portal.

2. The PKI portal responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest authentication.

3. The UE will generate the HTTP request by calculating the Authorization header values using the bootstrapping transaction identifier (B-TID) it received from the BSF as username and the NAF specific session key Ks_NAF.

If the certificate request needs extra assurance by a WIM application for key proof-of-origin, the UE generates a WIM challenge request containing parameters needed for key proof-of-origin generation [14].

4. The UE sends HTTP request to the PKI portal and includes the WIM challenge request in this request.

5. When the PKI portal, acting as an NAF, receives the request, it will verify the Authorization header by fetching the NAF specific session key Ks_NAF from the BSF using the B-TID, then calculating the corresponding digest values using Ks_NAF, and finally comparing the calculated values with the received values in the Authorization header. If the verification succeeds and the extra assurance for WIM application is needed, the PKI portal may use the PKI portal specific user security setting to compute the WIM challenge response [14].

6. The PKI portals send back a WIM challenge response containing additional parameters that are needed for the following PKCS#10 request generation. The PKI portal may use session key Ks_NAF to integrity protect and authenticate this response.

7. The UE will then generate the PKCS#10 request and send it to the PKI portal by using an HTTP Digest request. In the case that the private key is stored in a WIM application the ME should request the AssuranceInfo from the WIM application and include it in the PKCS#10 request, if provided. The enrolment request will follow the PKCS #10 certificate enrollment format as defined in [1]. Adding AssuranceInfo in this request is defined in the OMA ECMA Script specification [14]. The AssuranceInfo provides a proof of origin for the key processing.(e.g. identifies the WIM application and provides a proof that the key is stored in it). UE may indicate the desired format of the certification response: a certificate, a pointer to the certificate (e.g., URL), or a full certificate chain (i.e., from the issued certificate to the corresponding root certificate).

8. The enrolment request shall be as follows:

   POST <base URL>?response=<indication>[other URL parameters] HTTP/1.1
   Content-Type: application/x-pkcs10

   <base64 encoded PKCS#10 blob>

   where:

   <base URL> identifies a server/program.
   <indication> used to indicate to the PKI portal what is desired response type for the UE. The possible values are: "single" for subscriber certificate only, "pointer" for pointer to the subscriber certificate, or "chain" for full certificate chain.

   [other URL parameters] are additional, optional, URL parameters.

9. The incoming PKCS#10 request is taken in for further processing. If the PKI portal is actually a registration authority (RA), the PKCS#10 request is forwarded to CA using any protocol available (e.g., CMC as specified in IETF RFC 2797 [22] or CMP as specified in IETF RFC 2510 [2] and IETF RFC 2511 [3]). After the PKCS#10 request has been processed and a certificate has been created, the new certificate is returned to the PKI portal. It will generate a HTTP response containing the certificate, or the pointer to the certificate as defined clause 7.4 of WPKI [9], or a full certificate chain from issued certificate to the root certificate.

10. If the HTTP response contains the subscriber certificate itself, it shall be base64 encoded, and it may be demarcated as follows:

    HTTP/1.1 200 OK
    Content-Type: application/x-x509-user-cert

    -----BEGIN CERTIFICATE-----
    <base64 encoded X.509 certificate blob>
    -----END CERTIFICATE-----

    If the HTTP response contains the pointer to the certificate, the CertResponse structure defined in subclause 7.3.5 of the OMA WPKI [9] shall be used, and it may be demarcated as follows:

    HTTP/1.1 200 OK
    Content-Type: application/vnd.wap.cert-response

-----BEGIN CERTIFICATE RESPONSE-----
<base64 encoded CertResponse structure blob>
-----END CERTIFICATE RESPONSE-----

If the HTTP response contains a full certificate chain in PkiPath structure as defined in [15] and it shall be base64 encoded:

HTTP/1.1 200 OK
Content-Type: application/pkix-pkipath

<base64 encoded PkiPath blob>

The content-type header value for the certificate chain is "application/pkix-pkipath" as specified in [15].

The PKI portal may use session key Ks_NAF to integrity protect and authenticate the response, if a certificate or a pointer to the certificate is sent to the UE. The PKI portal shall use integrity protection and authenticate the response if full certificate chain is sent to the UE.

11. When UE receives the subscriber certificate or the URL to subscriber certificate, it is stored to local certificate management system.

NOTE: On board key generation is already defined in the WIM specification [8] issued by Open Mobile Alliance (OMA) group.

4.6.2 CA Certificate delivery

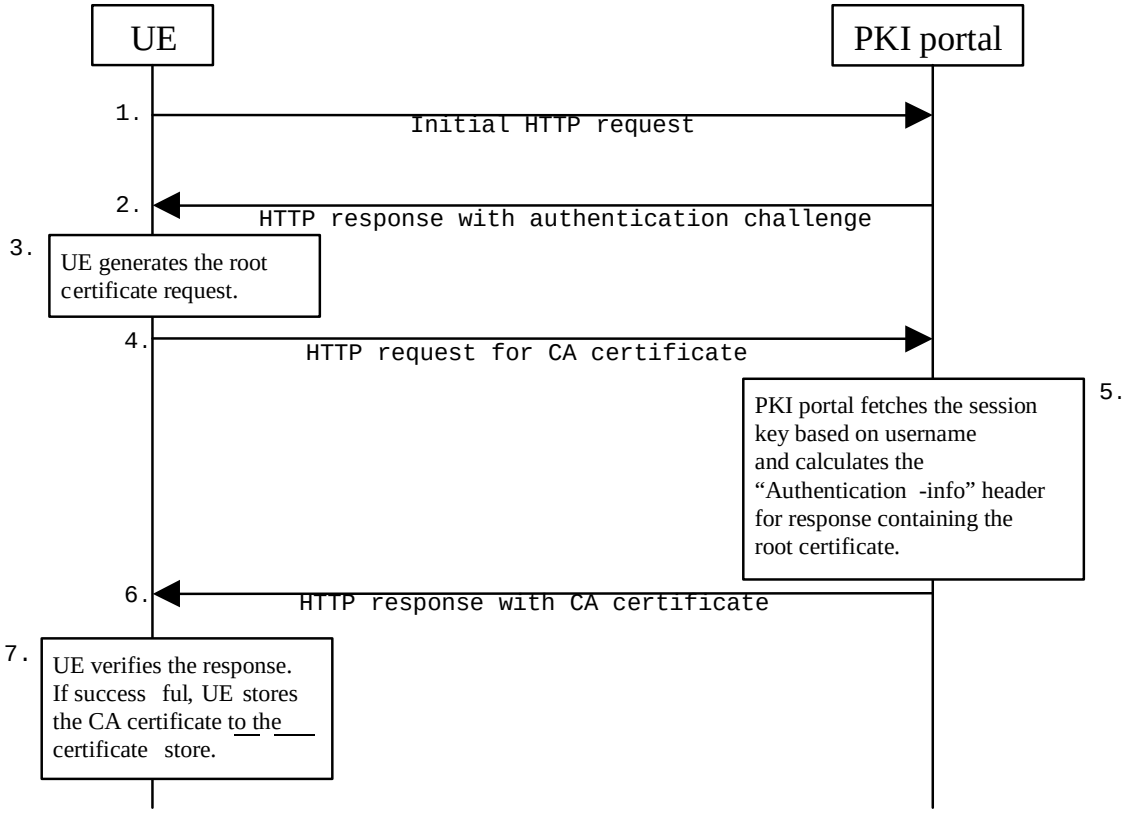

Figure 3: CA certificate delivery with HTTP Digest authentication

The sequence diagram above describes the CA certificate delivery when using HTTP Digest authentication. The procedure is secured as specified in clause 5.2 of TS 24.109 [20]. The detailed definition of the messages is left to stage 3 specifications.

1. The sequence starts with an empty HTTP request to the PKI portal.

2. The PKI portal responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest for authentication.

3. The UE generates another HTTP request for requesting the CA certificate. UE shall indicate the CA issuer name in the request URL as specified in subclause 7.4.1 of WPKI [9]. The serial number field shall be omitted. The Authorization header values are calculated using the identifier and the session key Ks_NAF. The authentication of this HTTP request is not necessary, but it is done in order to follow HTTP Digest authentication specification. Also, the identifier needs to be transported to the PKI portal.

4. The CA certificate delivery request shall be as follows:

   GET <base URL>?in=<issuer name>[other URL parameters] HTTP/1.1

   Where:

   <base URL> identifies a server/program.
   <issuer name> identifies the certificate issuer. It is a base64 encoding of the DER encoded Issuer field in the X.509 certificate.
   [other URL parameters] are additional, optional, URL parameters.

5. When the PKI portal receives the request, it may verify the Authorization header by fetching the session key Ks_NAF from the bootstrapping server using the identifier. The PKI portal will generate a HTTP response containing the CA certificate and use the session key Ks_NAF to authenticate and integrity protect the HTTP response using the Authentication-info header. Essentially, the response could also be other delivery protocol in HTTP format, e.g. PKCS#7 cryptographic message with content type signedData.

6. HTTP response contains the CA certificate. The CA certificate shall be base64 encoded, and it may be demarcated as follows:

   HTTP/1.1 200 OK
   Content-Type: application/x-x509-ca-cert

   -----BEGIN CERTIFICATE-----
   <base64 encoded X.509 certificate blob>
   -----END CERTIFICATE-----

7. When UE receives the new CA certificate, it must validate the Authentication-info header. If validation succeeds, the user is notified that a new CA certificate is taken into use. If user accepts the new CA certificate, it is stored to the local certificate management system and marked as "trusted" CA certificate.

4.7 Functionality in presence of pre-certified key pair or pre-shared keys

4.7.1 Presence of pre-certified key pair

An alternative to securing certificate enrolment based on AKA and bootstrapping function is to secure certificate enrolment based on signatures made with pre-certified key in the UE. This alternative has been specified by Open Mobile Alliance (see section 7.3.4 of WPKI [9]) and is thus out of scope of this specification. The functionality in presence of pre-certified key pair in the UE is explained below only briefly.

In this alternative solution, the UE equipped with a UICC, is previously issued with a pre-loaded, long lasting, public/private key pair from the home network. This phase would occur out of band, and would result in the UE possessing a long lasting key pair stored in the UICC for the purposes of certificate request authentication. Open Mobile Alliance (OMA) group offers standardized solutions by means of WPKI specification [9] and WIM specification [8] for the storage and the use of long-lasting key pair. USIM and WIM are examples of applications on the UICC that can deal with the long-lasting keys.

The UE can issue a request for a certificate to the CA, including a proof of origin (e.g. private key is stored in WIM) by using an administrative long lasting private key. The certificate request itself could contain a newly generated public key that is to be certified by the CA. This assumes that the new key pair is generated in the UICC. Access control security for the pre-loaded long-lasting private key should be at least as good as for access control for USIM.

The certificate for the administrative long lasting private key, that provides the proof of generated key origin, is always long lasting certificate. On the other hand the generated user keys in the WIM may have short or long-lived certificate depending on CA policies (see OMA's WIM [8], WPKI [9] and ECMA script [14] specifications).

4.7.2 Presence of symmetric pre-shared key

Same as above but the administrate key that provides the proof of generated key origin is a shared symmetric key, in which case it does not have a certificate (see OMA's WIM [8], WPKI [9] and ECMA script [14] specifications).

NOTE: The pre-shared symmetric key discussed in this chapter is not the same as the shared key associated with GBA.

Annex A (informative): Key pair storage

A.1 Introduction

The storage of the public/private key pair associated to the requested subscriber certificate is relevant to the procedure of issuing subscriber certificates.

The key pair storage can be performed in different ways. The nature of this storage may have impacts on the trust level associated to the subscriber certificates.

This annex provides a key pair storage security risk analysis in different scenarios.

A.2 Key pair storage use-cases

There are different scenarios to store the public/private key pair associated to the requested subscriber certificate.

A.2.1 Key pair storage on the ME

A possible place for the storage of the key pair is the Mobile Equipment.

There are two alternatives for the key pair storage on the ME: key pair storage on the MT or on the TE.

A.2.2 Key pair storage on the UICC

Another solution for the storage of the key pair is the UICC.

For the following study we will consider only two key pair storage use-cases: on the ME or on the UICC.

A.3 Threats associated with the key pair

A.3.1 Key pair generation

The key pair generation is a very sensitive operation for the secrecy of the private key. The key pair generation has to be of good quality and the exchange, between the device where the key pair generation took place and the device where the key pair will be stored, has to be protected to avoid private key cloning/disclosure. UICC provides a greater level of protection, compared to ME, against unauthorized access to the private key itself.

A.3.2 Unauthorized usage of the private key

There are two kinds of threats associated with unauthorized usage of the private key:

1. An attacker getting hold of the private key; and
2. An attacker using the private key of the victim without getting hold of that key.

With respect to threat 1, having the key in UICC offers better protection than having it in the ME. However, an attacker who can compromise the ME can possibly *use* the private key for unauthorized purposes even if it is in the UICC because the UICC does not have direct trusted path to the user.

Attacks due to threat 2 always require an interaction with the UE to gain access to the UICC. While with the threat 1, as soon as the key is retrieved, the associated attacks do not requires any interaction with the UE to use the retrieved private key.

A.3.3 Portability

If the key pair is stored on the Mobile Equipment there is a threat in case of a new UICC inserted in this ME. There will be on the ME personal and sensitive data that do not belong to the new user. Since access to private keys is protected by PINs or passwords, the new user cannot access the private key of the old user unless he knows the PIN or the password.

Also, an important aspect of enrolling subscriber certificates based on AKA is the use of short-lived certificates. With short-lived certificates, even if the new user can access the old user's private key, it could happen that he cannot masquerade as the old user in authorization transactions because he can no longer get subscriber certificates for the key pair on behalf of the old user if the subscriber certificate expired. Moreover, if the key pair in ME is short-lived, owner of the new UICC will not be able to use that key pair after the pair expires. But there is no assumption that the subscriber certificate/key pair expired when the new user gets access to the old user's private key. In general, short-lived keys – on UICC or on ME – are useful for identity and privacy protection. Frequent change of key pair prevents outsiders from linking together transactions made by same user.

A.3.4 Environment

The threats to the key pair depend on the environment, the place of the key pair storage.

All implementations on mobile terminal, PC, MAC or PDA leave potential risks such as the possibility to load Trojan horses, worms or virus. Software applications lack the protective mechanisms existing in smart card (tamper resistance, physical encapsulation of critical circuitry). Reverse engineering techniques, such as extracting program code and disassembly/debugging methods, are simplified greatly in a software environment, allowing a token's secret components such as cryptographic algorithms, private keys, and other assumed secure information to be recovered.

Currently, the Mobile Equipments do not have all the hardware and software countermeasures that are built into UICC to protect them against invasive and non-invasive attacks performed to retrieve secrets. But mechanisms like code signing are already being taken into use.

A.3.5 Threat to the required properties for digital signatures

To be valid, digital signatures require the following properties:

- Authenticity: a valid signature implies that the signer deliberately signed the associated message;
- Unforgeability: only the signer can give a valid signature for the associated message;
- Non-re-usability: the signature of a document can not be used on another document;
- Non-repudiation: the signer can not deny having signed a document that has valid signature;
- Integrity: ensure the contents have not been modified.

Those properties involve the secrecy of the keying material, having a trusted input/output path to the user, and the use of strong and secure cryptographic mechanisms.

So, the trust in the digital signatures depends on the storage of the key pair and the related cryptographic computations and the security of communication between the user and the module performing private key operations. The impacts of the key pair storage are studied in the following clause A.4.

A.4 Security risk analysis related to key pair storage

There are many different subscriber use-cases describing the range of applications or services utilizing subscriber certificates. But, the level of trust associated to the proposed services depends on the key pair storage. This will be presented in the following security risk analysis.

A.4.1 Subscriber certificate use-cases

The use-cases for subscriber certificates can be divided into 2 main categories:

A.4.1.1 Secure services

Those services provide convenient way of authenticating cellular subscribers to services. These services can be provided by cellular operators, corporations, or 3rd party content providers. Secure services may also support billing.

The different subscriber use-cases could be:

- person-to-person authentication: per-to-per authentication;
- corporate services: 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.

A.4.1.2 Secure connectivity

This service utilizes cellular infrastructure and existing operators customer relationships to authenticate users:

- alternative access authentication:
  - corporate WLAN access authentication;
  - broadband access, e.g. DSL or cable access;
- service authentication: e.g. VPN authentication.

A.4.2 Security risk analysis in some scenarios

All subscriber use-cases do not require the same level of security for the key pair storage since they propose services that have different features in terms of:

- added value: high or low valued services;
- involved partners and trust relationships: there is agreement between different cellular network operators or between cellular network operator and service provider or 3rd party content provider;

- type of required certificates (short-lived or long-term certificates).

This section presents some scenarios where the nature of the key pair storage has security impacts on the service.

A.4.2.1 Scenarios involving subscriber's personal data

An example of scenario involving subscriber's data could be the self-service management.

A.4.2.1.1 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.

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.

A.4.2.1.2 Security Risk Analysis in this scenario

The security risk analysis is performed according to the unauthorized usage threats identified in clause A.3.2.

Unauthorized usage by using the private key of the victim without retrieving the private key:

Potential attack:

so, an attacker could get usage of the subscriber private key to authenticate to the Web portal and access for self-provisioning. The attacker could for example modify the subscription profile of the subscriber.

Feasibility:

the attacker requires an interaction with the UE to gain access to the UICC.

the attack applies in case of:

- key pair storage on the ME;
- key pair storage on the UICC.

Unauthorized usage by getting hold of the private key:

Potential attack:

so, an attacker could retrieve the subscriber private key to authenticate to the Web portal and access for self-provisioning. The attacker could for example modify the subscription profile of the subscriber.

Feasibility:

once the key retrieved, the attacker does not require any interaction with the UE equipment to gain access to the UICC.

the attack applies in case of:

- key pair storage on the ME

  This attack is based on the key retrieval. So, as the UICC is tamper resistant device so the attack does not apply to UICC.

Consequences of these attacks:

the self-service management is low added value and the consequences of the key pair storage on the UE are limited.

A.4.2.2 Scenarios involving payment and agreement between operator and service provider

Some scenarios deal with payment and agreement between cellular network operator and service provider, 3rd party.

A.4.2.2.1 Notifications through cellular network scenario

The 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 notification through his phone bill. Subscriber authorizes such payment and the charging is triggered when the service provider sends a notification.

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.

A.4.2.2.2 Small to medium payment through cellular operator 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 information in the certificate, then the subscriber may remain anonymous towards the service provider. The service may be e.g. non-cellular access in a environment where the operator's traditional billing mechanisms are not directly applicable, e.g. non-cellular access is provided by 3rd party.

During a payment transaction the 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).

Prerequisite:

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.

A.4.2.2.3 Security Risk Analysis in these scenarios

These secure services deal with payment and an agreement between a cellular network operator and a service provider. The nature of the key pair storage has consequences. The security risk analysis is performed according to the unauthorized usage threats identified in clause A.3.2.

Unauthorized usage by using the private key of the victim without retrieving the private key:

Potential attacks:

if the ME is not sufficiently secure, the attacker may have a program that shows the user a certain message ("payment of €1") but ask the UICC to sign a different message ("payment of €100). Also if the attacker's program discovers the PIN, it can command the UICC to generate signatures even without the user being aware of it.

Feasibility:

the attacker requires an interaction with the UE to gain access to the UICC.

these attacks apply in case of:

- key pair storage on the ME;
- key pair storage on the UICC.

Unauthorized usage by getting hold of the private key:

Potential attacks:

if an attacker manages to discover the subscriber's private key then an attack could consists in sending signed authorizations to the service provider, then the subscriber would have to pay for services he did not ask for.

Feasibility:

once the key retrieved, the attacker does not require any interaction with the UE equipment to gain access to the UICC.

The attack applies in case of:

- key pair storage on the ME.

This attack is based on the key retrieval. So, as the UICC is tamper resistant device so the attack does not apply to UICC.

Consequences of these attacks:

- forgeability: the subscriber could pay for services he did not ask for;
- repudiation: The cellular network operator and the service provider are not paid for the service they provided.

  If there is any way to attack the system a signer can repudiate the performed signatures arguing that the system is not secure. So, if it is possible to use the subscriber's private key without his deliberate consent, then the subscriber can repudiate the signatures sent for authorization, and not pay the associated phone bill. So,:

  - the operator and the service provider could not be paid for the proposed service;
  - the trust relationship between the operator and the service provider can be destroyed. The service provider has no guaranty of security; he would no longer trust the subscriber certificates issued by the cellular network operator and the associated signatures;

- if there is any problem due to some unauthorized usages of the subscriber private key then the trust in 3G PKI may be lost;
- high valued services involving payment and relationship with service provider or 3rd party content provider often require the use of long-term certificates. The issuance of long-term certificates requires more security constraints than the issuance of short-lived certificates. So, according to the unauthorized usage threats present on the UE, the security level may not satisfy the security requirements for long-term certificates issuance and usage.

A.4.3 Summary of risk analysis

To prevent the identified unauthorized usages of the private key the following recommendations need to be addressed:

- the storage of the private key and the related cryptographic computations to be done in a secure manner;
- the solution should provide a secure path to the private key usage.

The UICC provides the most secure location for storage and usage of the private key in terms of security (in the form of, e.g. the WIM application). This does not preclude the use of other locations for certain services. On the other hand, the ME can provide a secure path to using the private key (e.g. with mechanisms such as code signing). The combination of solutions will provide a complete secure solution and enable the deployment of secure services.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-03	SP-23	SP-040165	-	-	Presented for approval at TSG SA #23	1.2.1	2.0.0
2004-03	SP-23	-	-	-	Approved and placed under Change Control (Rel-6)	2.0.0	6.0.0
2004-09	SP-25	SP-040620	0001	-	User security settings	6.0.0	6.1.0
2004-09	SP-25	SP-040620	0002	-	Editorial cleanup	6.0.0	6.1.0
2004-09	SP-25	SP-040620	0003	-	Cleanup of procedure descriptions	6.0.0	6.1.0
2004-09	SP-25	SP-040620	0004	-	Removal of unnecessary editor's notes	6.0.0	6.1.0
2004-12	SP-26	SP-040856	0005	-	Visited network issuing subscriber certificates	6.1.0	6.2.0
2004-12	SP-26	SP-040856	0006	-	Editorial correction	6.1.0	6.2.0
2006-03	SP-31	SP-060053	0007	-	Update PSK TLS Reference	6.2.0	6.3.0
2007-06	SP-36	SP-070328	0008	-	Removal of editors note	6.3.0	6.4.0
2007-06	SP-36	-	-	-	Update to Rel-7 version (MCC)	6.4.0	7.0.0
2007-12	SP-38	SP-070787	0009	-	Usage of OMA References – Update of References	7.0.0	7.1.0
2008-12	SP-42	--	--	--	Update to Rel-8 version (MCC)	7.1.0	8.0.0
2009-12	SP-46	-	-	-	Update to Rel-9 version (MCC)	8.0.0	9.0.0
2010-06	SP-48	SP-100361	0010	1	Deprecation of SHA-1 and other changes to certificate and CRL profiles	9.0.0	9.1.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.1.0	10.0.0
2012-09	SP-57	SP-120605	0011	-	Deletion of unused references	10.0.0	11.0.0
2012-10					Editorial changes	11.0.0	11.0.1
2013-12	SP-62	SP-130662	0012	1	CR to TS 33.221 Correction of Reference	11.0.1	11.1.0
2014-09	-	-	-	-	Update to Rel-12 version (MCC)	11.1.0	**12.0.0**
2016-01	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	**13.0.0**

History

Document history		
V13.0.0	January 2016	Publication