3GPP TSG SA WG3 Security — S3#23 **S3-020300**
14 - 17 May 2002, Victoria, Canada

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.102** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **4.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Support for certificates
Source:	⌘	Nokia
Work item code:	⌘	***Date:*** ⌘ 7. May 2002
Category:	⌘	**B** ***Release:*** ⌘ 6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	Adding a feature according to the corresponding work item
Summary of change:	⌘	Adding the description of the feature in section 5.4; adding the desciption of the corresponding mechanism in section 6.7; adding description of certificates in Annex D
Consequences if not approved:	⌘	The planned feature is not specified.

Clauses affected:	⌘	5.4.2 , 6.7, Annex D		
Other specs affected:	⌘	**X** Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	24.008
Other comments:	⌘			

5.4 Application security

5.4.1 Secure messaging between the USIM and the network

USIM Application Toolkit, as specified in 3G TS 31.111 [15], provides the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider.

Security features for USIM Application Toolkit are implemented by means of the mechanisms described inTS 23.048 [7]. These mechanisms address the security requirements identified in GSM 02.48 [16].

5.4.2 Void

5.4.3 Void

5.4.4 Void

5.4.5 Support for certificates

There exists a need for a global scale authorization infrastructure for various applications and services. This may be based on the 3GPP system security architecture. Many of these emerging services will be provided by parties that are not necessarily trusted by the cellular operators nor by cellular subscribers. Therefore technical means to deal with, and preferably minimize, disputes between subscribers and service providers is necessary. Authorization of such services may be based on credentials like digital signatures. The service provider shall use subscriber certificates in verifying credentials. The UE may also use certificates of operators (operator certificates) and other certificates issued by operators in verifying credentials supplied by service providers.

The core network shall provide support for issuing certificates to the UE over the authenticated network connection between the ME and the core network. Clause 6.7 describes mechanisms to provide this support.

****** NEXT MODIFIED SECTION*******

6.9 Support for delivering certificates

The delivery of certificates shall be performed as follows. There are two separate procedures: one for issuing subscriber certificate and another for delivering operator certificates. Both are run between the UE and the CN of the serving network. The CN contains the Certification Authority (CA) functionality. The certificate messages are authenticated because they are sent over integrity protected signalling channel.

Subscriber certificates issued in this manner are authorisation certificates. They do not necessarily certify identities.

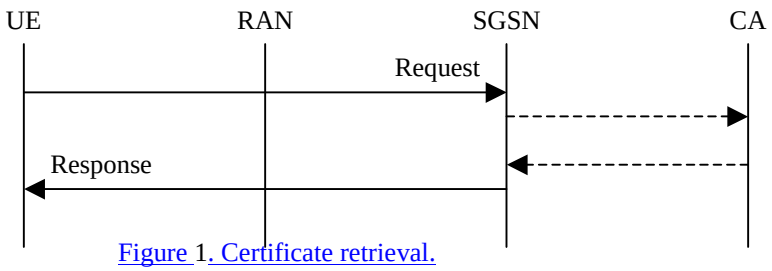

Figure 1. Certificate retrieval.

In the case of requesting a subscriber certificate, the request shall contain information about what needs to be certified (e.g., a public key). The response shall contain one of the following:

- a subscriber certificate itself, or
- an address from which the UE shall obtain the subscriber certificate, or
- an address which the service provider may use in verifying the credentials supplied by UE, or
- an error message.

In the case of retrieving the operator certificate, the request may contain information that explicitly identifies a particular operator which may be different from the visited operator. The response shall contain one of the following:

- the operator certificate itself, or
- information needed to verify the operator certificate, and an address from which the UE shall obtain the operator certificate, or
- an error message.

Further details see annex D.

~~e use tunderlinedunless another reference is explicitely specified.~~

~~*MacKey()*mustmustmust~~

***** NEXT MODIFIED SECTION *****

Annex H: (normative) Support for certificates

This annex defines the certificate related parameters used in procedures of clause 6.7.

The following typographic convention:

- Names of information element fields in protocol messages are bold italic.
- Names of types are italic.
- Optional fields are marked “(OPTIONAL)”
- Message parts marked “(CRITICAL)” require integrity protection. Message parts marked “(NON-CRITICAL)” do not require integrity protection. See more discussion on this aspect below.

Definitions of composite types mentioned in this section can be found in [CERT-FORMAT]. Both protocols are of a simple request/response type as shown in clause 6.9.

H.1 Subscriber Certification

Request: (CRITICAL)

- ***key-info****: choice* of
  - ***public key***: *SubjectPublicKeyInfo* (algorithm identifier, and bitstring)

- ***pk_hash***: *KeyIdentifier* (octet string; algorithm is SHA-1)

- ***key-origin***: *byte*, with e.g. the following reserved values
  - 0 = from UICC, 1 = from another security module on UE, 2 = from outside UE, 3 = from UE own memory

- ***intended-key-usage***: *Boolean* flag describing which usages are proposed, with the following values: 0 = automatic signing allowed 1 = signing with explicit user confirmation only

- ***user-plane-continuation-capability***: *Boolean* flag. Should be set to true only if the terminal can accept a continuation URL (see the Response definition below).

- ***device-certificate***: *Certificate* (OPTIONAL); certificate issued by the manufacturer of the device where the private key resides (e.g., a smartcard).

Response: (NON-CRITICAL)

- ***cert-info***: *choice* of
  - ***subscriber certificate***: *Certificate, WAPCertificate* [WAPCert]
  - ***subscriber certificate URL***: *URL* formatted as specified in [WPKI, section 7.3] from which the certificate can be retrieved. The UE will give this URL to the verifier instead of its certificate
  - ***failure***: *sequence* of
    - ***error***: *byte*, with e.g. the following reserved values
      1. unknown cause
      2. continuation requested (continuation URL shall be present below)
      3. service not available (this network does not issue certificates)
      4. service not available now (try later)
      5. service not possible without user-plane continuation (if terminal indicated user-plane-continuation-capability=false)
      6. key-origin not acceptable
      7. device certificate required (resend certificate request with the device certificate attached).
      8. device certificate invalid (e.g., expired, incorrect, or otherwise invalid)
  - ***continuation URL***: *URL* (OPTIONAL)

H.2 Operator certificate retrieval

When a successful response for the subscriber certification request is received, UE will find the Issuer Name of the operator CA. It can use this to check if it already has a valid certificate for the operator CA's public key. If not, it can initiate the operator certificate retrieval protocol below.

A second scenario for operator certificate retrieval is when a service provider specifies the operator (by e.g. specifying the hash of the operator CA's public key) in application-layer signalling. In this case, the UE will know the key hash of the operator but may not know the Issuer Name.

The operator certificate retrieval protocol is as follows:

Request: (NON-CRITICAL)

- ***target***: (OPTIONAL) *choice* of
  - *Name*. Distinguished name of the issuing operator.
  - *KeyIdentifier* (octet string, algorithm is SHA-1) of the operator CA's public key
- ***user-plane-continuation-capability***: *Boolean* flag indicating if the terminal can accept a URL of the operator certificate or not.

Response: (CRITICAL)

- ***operator-cert***: *X.509v3 certificate*
- ***failure***: *sequence* of
  - ***error***: *byte*, with the following reserved values
    1. unknown cause
    2. no matching certificate
    3. service not available now (try later)
    4. service not possible without user-plane continuation (if terminal indicated ***user-plane-continuation-capability***=false)
- ***operator cert-info***: (OPTIONAL) *sequence* of
  - ***hash***: *KeyIdentifier* (octet string, algorithm is SHA-1)
  - ***url***: *URL* of the operator certificate

H.3 References

[CERT-FORMAT] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459.

[WAPCert] WAP Certificate and CRL Profiles, WAP-211-WAPCert, Version 22-May-2001.