3GPP TSG SA WG3 Security — S3#23 **S3-020322**

14 - 17 May 2002

Victoria, Canada

Title: LS on subscriber certificates
Source: SA3
To: SA2, CN1
Cc: SA1

Contact Person:
Name: **Valtteri Niemi**
Tel. Number: + 358 50 48 37327
E-mail Address: valtteri.niemi@nokia.com

Attachments: S3-020077, S3-020300

---

1. Overall Description:

SA3 are working on a Release 6 work item called “Support for subscriber certificates”. The objective of the work is to create a security capability for 3GPP systems that can be used to provide secure mechanisms for various applications and services.

Some example usage scenarios for these certificates are described in the attached document S3-020077.

The core of the planned new functionality is described in the attached proposed CR to TS 33.102 (3G security architecture) NOTE: This CR has not yet been approved by SA3.

It is essential for the feature that integrity protected signalling channels can be used for certificate request-response procedures. This implies that the new procedures are included as part of the UE-CN signalling, and the two procedures are specified in TS 24.008.

It is not the intention of SA3 to specify a full public key infrastructure. Instead, existing components of e.g. Wireless PKI are re-used. This limits the amount and scope of the specification work needed in 3GPP. However, a so-called Certificate Authority (CA) is needed when certificates are issued. In the proposed mechanism, the cellular core network and the PKI are associated to each other via a link between SGSN and CA.

2. Actions:

ACTION TO CN1: To study the impacts of the proposed mechanism to 24.008 and provide feed-back to SA3 as necessary;

ACTIONS TO SA2:

1. To study the impacts of the proposed mechanism to the 3GPP system architecture and provide feedback to SA3 as necessary.
2. To study the need of standardisation of the interface between SGSN and CA.

3. Date of Next TSG-SA3 Meetings:

SA3-24	9th – 12th July 2002	Helsinki, Finland
SA3-25	8th – 11th Oct 2002	Munich, Germany

3GPP TSG SA WG3 Security — S3#22 **S3-020077**

25 - 28 February 2002

Bristol, UK

Source: **Nokia**

Title: **Usage scenarios for subscriber certificates**

Document for: **Discussion**

Agenda Item: **TBD**

1. Introduction

Certificates issued by the cellular network based on USIM authentication allow also service providers to access the population of cellular subscribers.

The concept offers new business opportunities for both operators and service providers. The operators have established a business infrastructure for authentication, authorization, and accounting of roaming subscribers. Issuing subscriber certificates allows operators to offer authorization and accounting as a value added service for providers of other services.

This document describes three example usage scenarios of the subscriber certificate feature. These are payment via subscriber phone bill, notification service offered by operator to other service providers and location information offered by the operator to other service providers. In addition to the usage scenarios described in this document subscriber certificates could be used in authorizing services provided by operator itself, e.g. to allow access with alternative wireless technologies like WLAN or Bluetooth.

In the payment scenario, the service providers offer their service to consumers and are reimbursed for the offered services by the cellular operator. This is attractive to service providers because they do not have to collect individual payments from users of their services. In effect, they outsource billing to cellular network operators. Moreover, service providers can do this without having to learn user's real identity or phone number, or credit card number.

In the other two scenarios, the offered service may require information, or action from the cellular network. An example of such information is the current physical location of the user's phone (and thus of the user). An example of an action is informing the user through a SMS (or other messaging mechanisms) sent by the cellular network and for which the user pays himself. To get the needed information or trigger action of the cellular network, the service provider needs a signed authorization from the user. He does not need to learn user's real identity or phone number to verify user's signature.

In the diagrams on the following pages, the Signalling Layer contains the implementation of the 3G standardized subscriber certificate feature and messaging. The Application Layer, utilizes the Signalling Layer. It could be, for instance, the combination of a browser and a plug-in which handles authorization of services and payments.

2. Acquiring a subscriber certificate

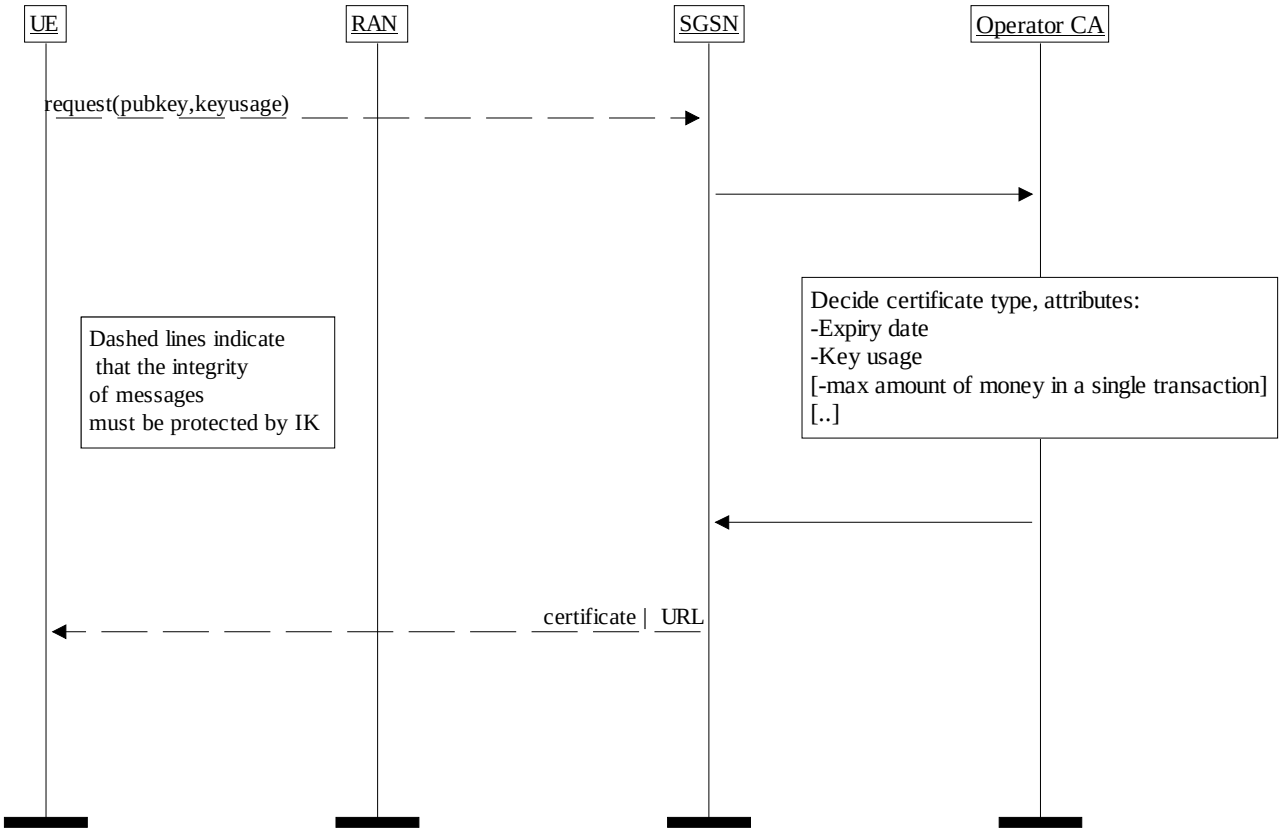

Fig 1: The certificate request scenario

Explanation of the diagram

Key usage describes what the key should be used for, e.g. authentication or signing. It is possible to define new key usage types such as restricting the certificate to non-monetary transactions.

A key point here is that subscriber certificates do not reveal the real identity of the subscriber: rather they provide an identifier which only the operator can map to the real identity.

Operator certificates can be retrieved similarly to subscriber certificates. The mobile terminal can use this certificate to enable authentication of its peer. A typical example would be when a UE establishes a TLS channel to a service provider.

3. Authorization of payment through phone bill

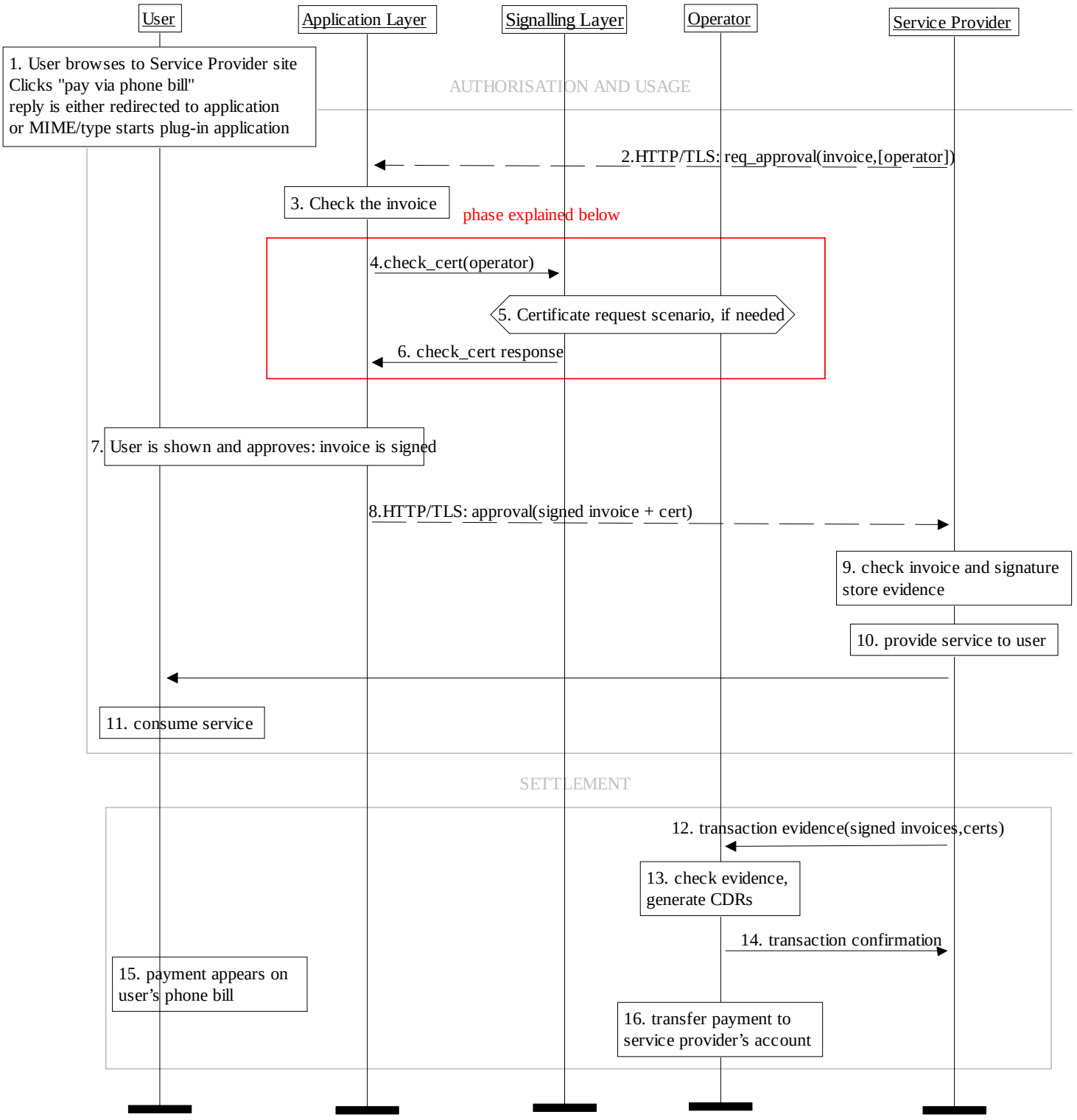

Figure 2: Payment via operator billing

Explanation of the diagram

The diagram shows 2 stages of payment for a service through the phone bill: authorization and usage (messages 2-16) and settlement (messages 17-21). Note that use of TLS is not necessary, but provides extra security by authenticating the server and encrypting the payment contract details.

1. Message 1: Using the browser on the phone (web or wap) the user visits a site which supports payment via operator phone bill. After selecting some products to purchase, the user clicks the link "pay via phone bill". The server prepares a payment contract and sends it as the response.

2. Messages 2-6: This phase covers the preparation of an invoice by the server, the issuing of subscriber certificate, if needed (message 4-6), and the presentation of the invoice to the user.

3. Messages 7-10: In this phase, the approved invoice is signed and delivered to the service provider together with the certificate. With the aid of the certificate, the service provider checks the invoice and the signature and stores the transaction evidence.

4. Message 11: The user gets the service.

5. Message 12-16 Settlement stage. The service provider delivers transaction evidence to the operator (message 12) who checks the evidence and generates CDRs (action13) and then transfers payment for the service to the service provider's account (action 16). After the CDRs are processed by the cellular infrastructure, the payment appears on the users phone bill (action 15).

4. Delivery of location information

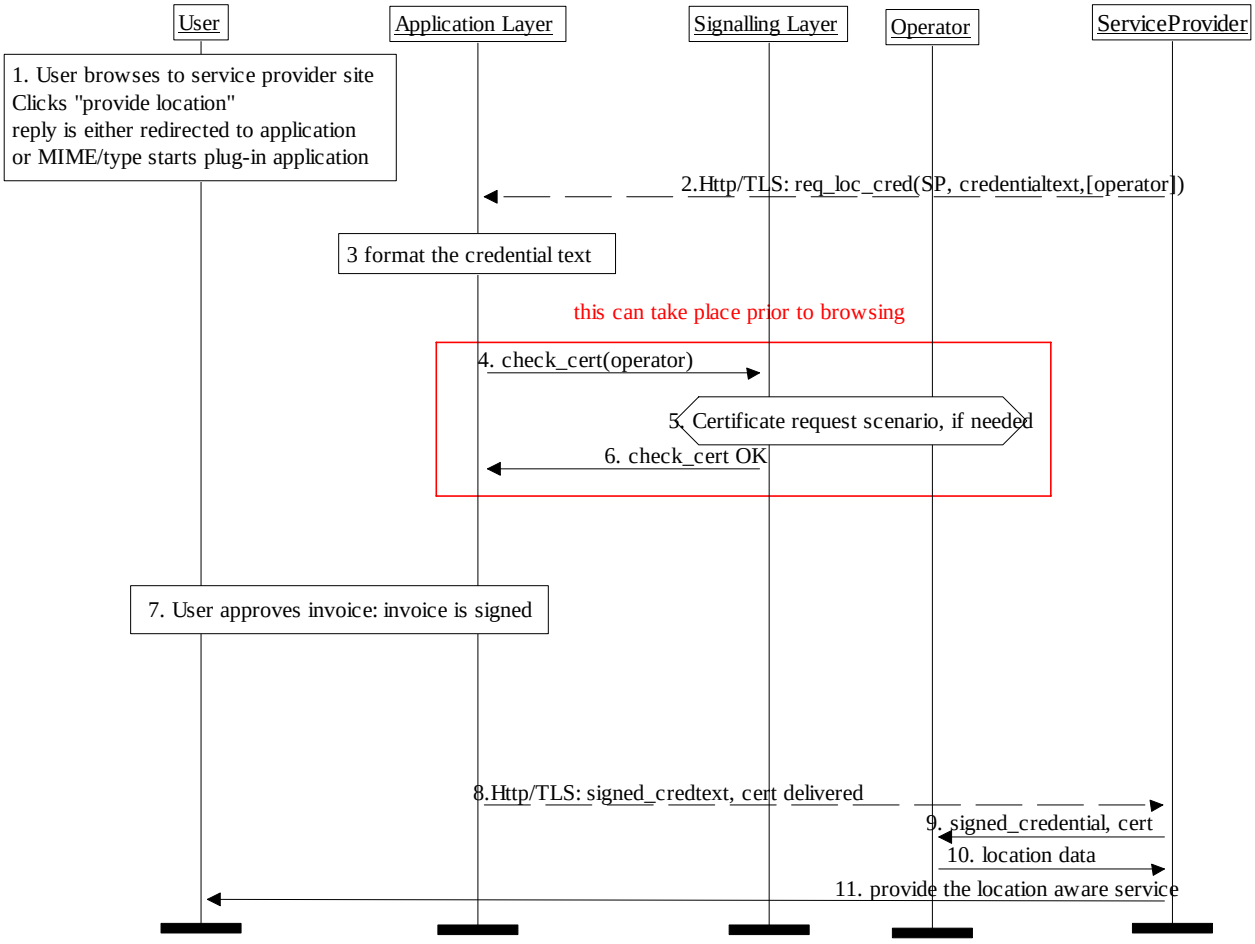

Figure 3: Delivery of location information

Explanation of the diagram

This scenario illustrates how the subscriber certificate is used to enable location-aware applications. Here credentials are used in place of invoices: the signed credential gives the service provider the right to obtain the user's location from the operator.

There are many similarities with the first scenario: the authorization stage is split into a number of steps:

1. Message 1: Using the browser, the user selects to reveal their location details to the service behind the web site they are currently browsing.

2. Message 2-6: The credential is created by the server and returned to the browser. The certificate is retrieved, if necessary, from the operator, otherwise from the certificate store on the device. The credential is formatted and presented to the user.

3. Messages 7-8: The approved credential is signed and delivered (along with the subscriber certificate) to the service provider.

4. Messages 9-10: The signed credential and certificate are submitted by the service provider to the operator, who responds with the location information (e.g. Cell ID)

5. Message 11: With the service provider knowing the location of the terminal, a localized service can be created for the user.

Other issues

Who pays for the service and how is an orthogonal issue. If the user pays for the service via operator billing, then the flow of this scenario overlaps with that shown in Section 2. It is also conceivable that the service is free for the user.

Why use certificates? In this scenario, certificates are useful in two cases:

- The operator server that issues certificates is different from the operator server that verifies credentials
- Operator does not want to store any data about user public keys and preferences.
- Non-repudiation.

An alternative approach could be to allow the terminal to send the Cell ID itself and bypass the operator query and signing issues. However, the Cell ID would be of limited use to the service provider without the ability to convert it into physical coordinates – something which may involve contact with network operator anyway.

5. Delivery of notification information

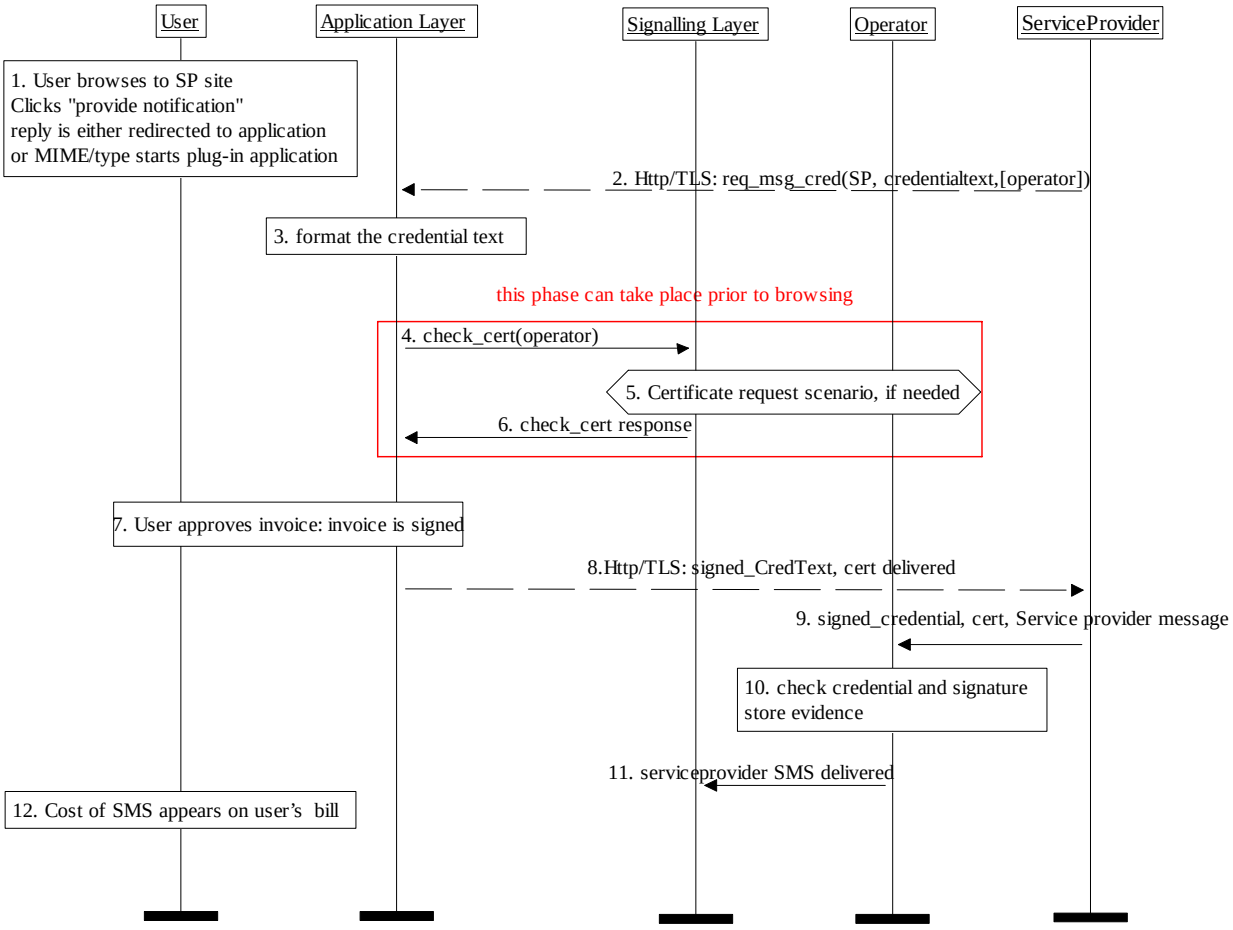

Figure 4: Delivery of notification information

Explanation

The message flow is very similar to the previous scenario. The credential approach is used to enable the user to request that a service provider will send messages to his phone. This can happen later when certain condition is fulfilled. The user meets the cost of sending these messages. User privacy is preserved as her MSISDN is not revealed to the service provider.

Messages 1-8 are the same as in the previous scenario.

After message 8, the service provider is in possession of a signed credential from the user which allows messages to be sent to that user via the operator. The messages are not sent directly to the user: the service provider has no access to his MSISDN. The service provider also has the user certificate.

Message 9 involves the service provider creating an SMS message to be sent to the user (e.g. breaking news about stock prices etc..) and sending this along with the signed credential and user certificate to the operator.

Message 10: The operator can verify the validity of the signed credential. If everything is in order the message is queued for sending and billing evidence is

generated to place the cost of the message onto the user’s phone bill. The operator can easily map the user certificate to the user MSISDN.

Message 11: The SMS arrives at the destination phone and later the user is billed.

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	⌘	24.008
		☐ Test specifications		
		☐ O&M Specifications		
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.

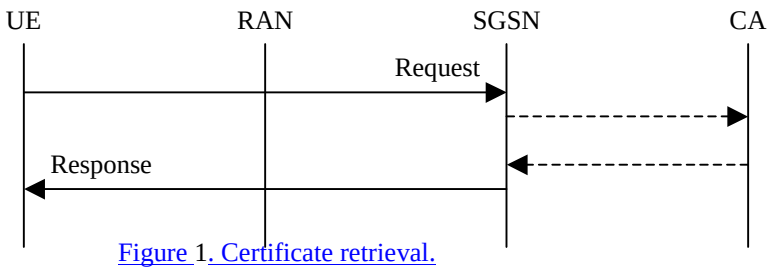

Figure 1. Certificate retrieval.

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.