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

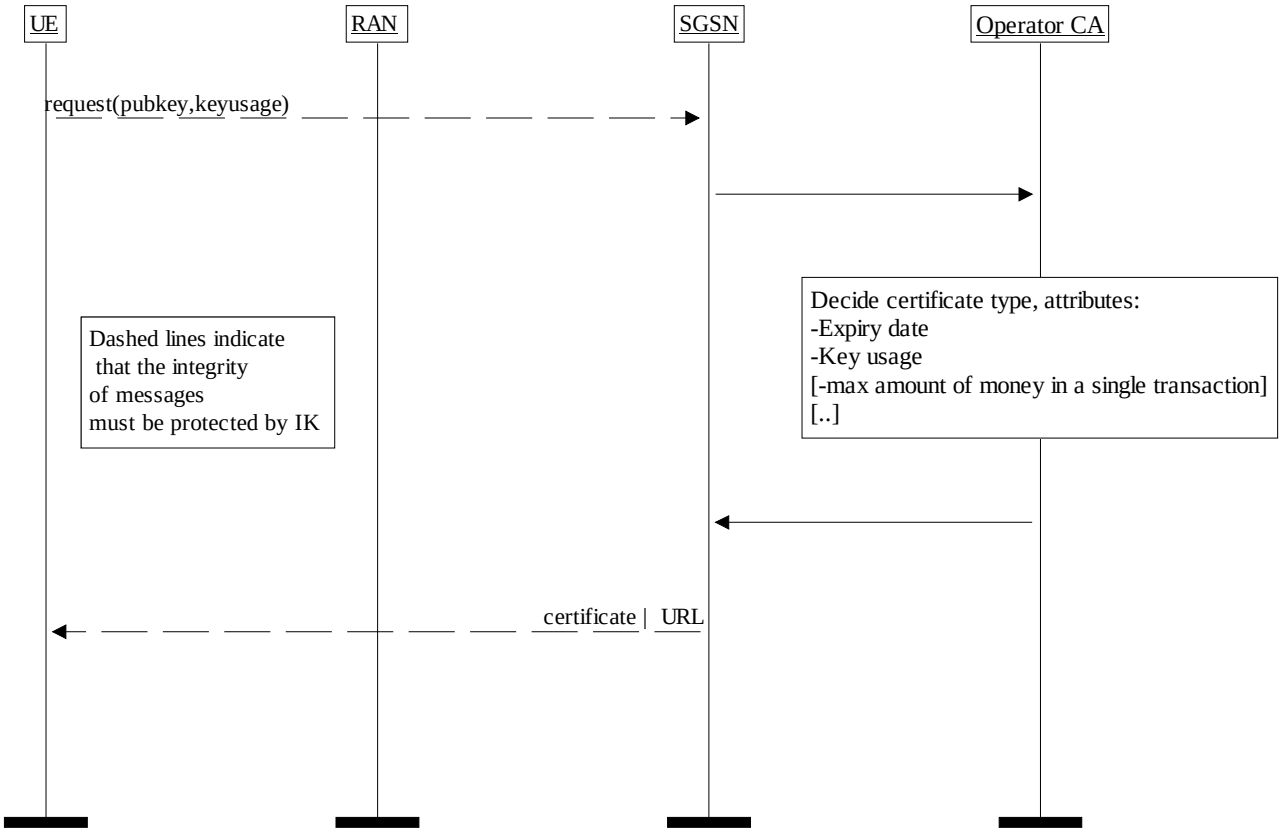

Fig 1: The certificate request scenario

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

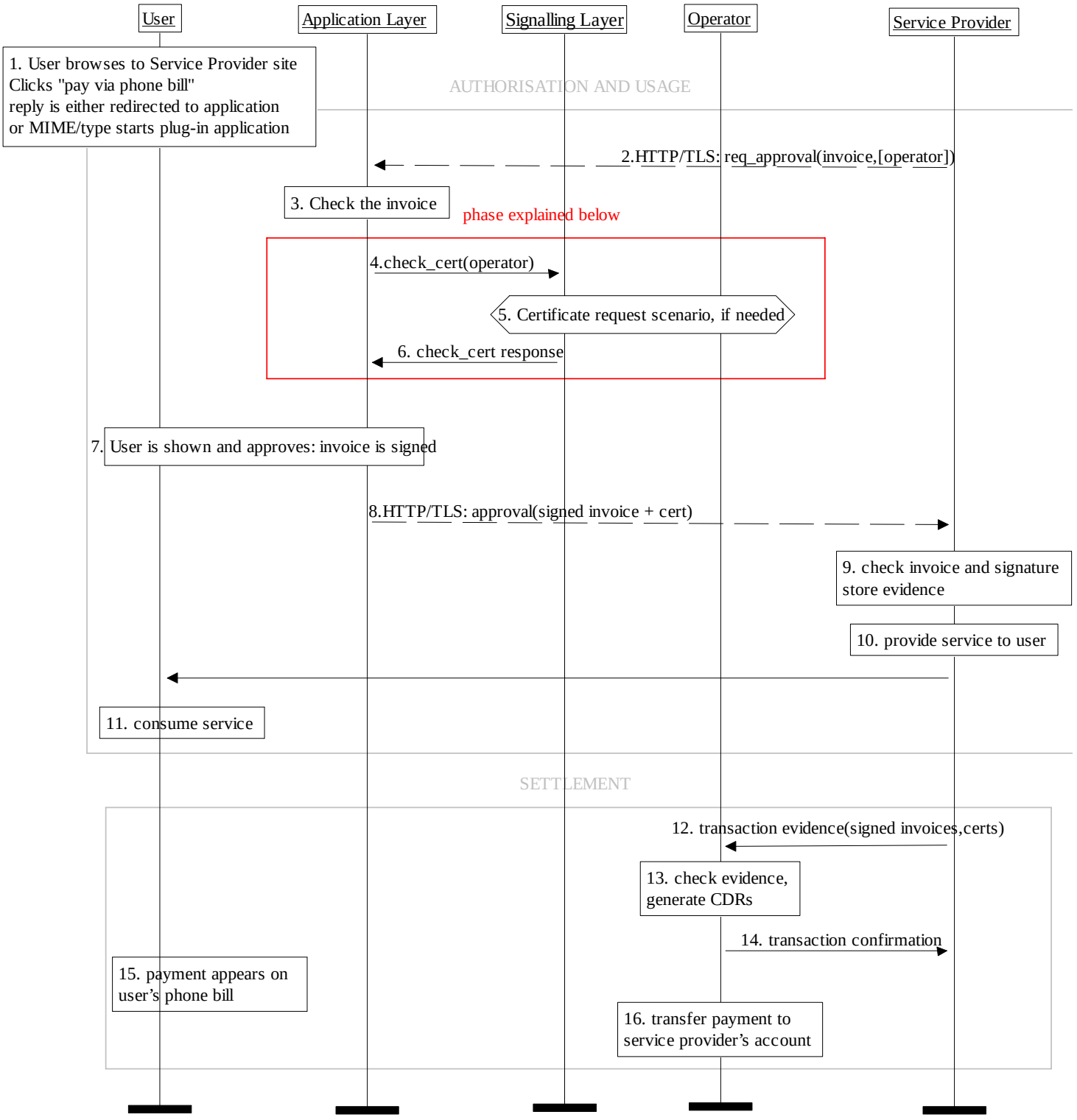

Figure 2: Payment via operator billing

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

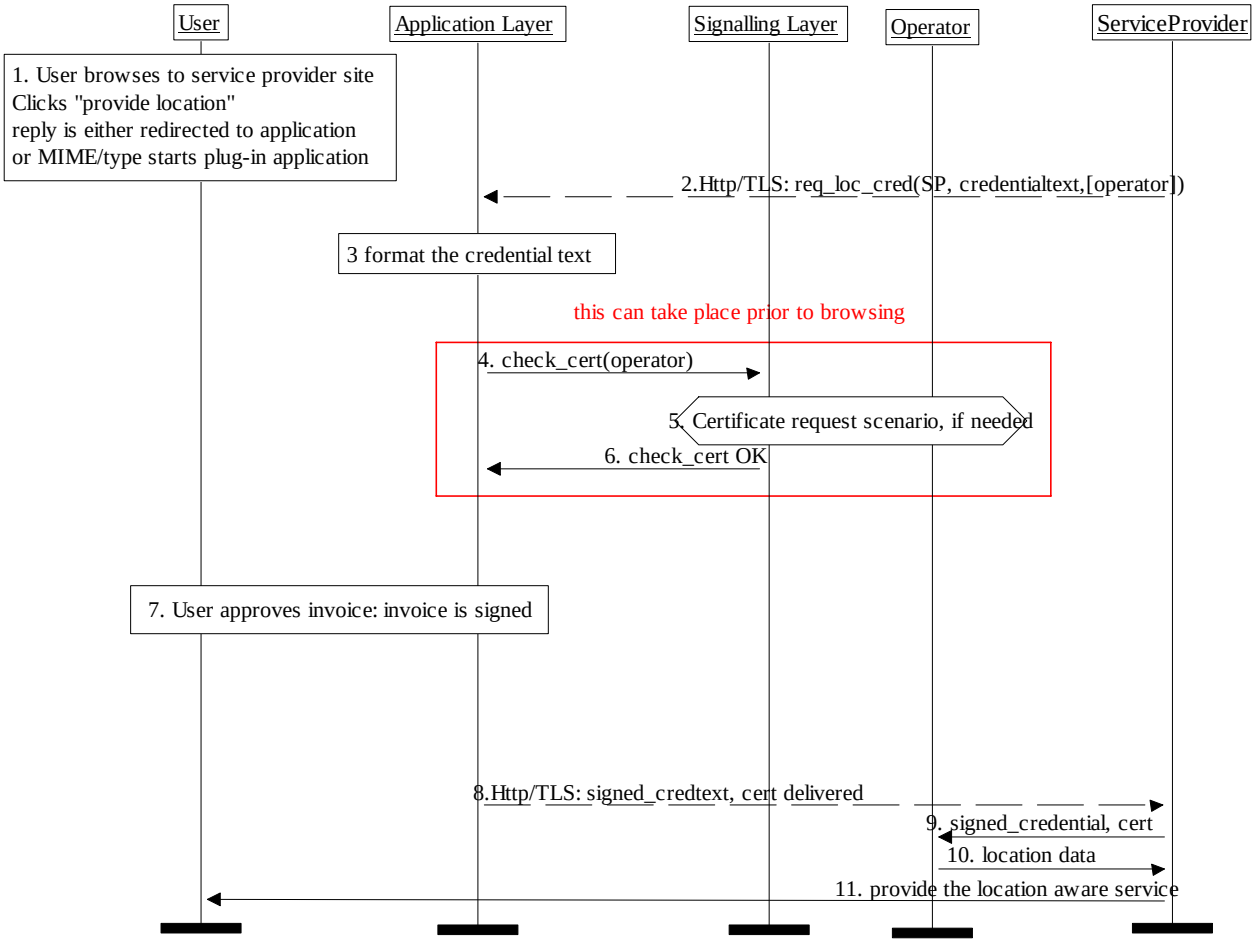

Figure 3: Delivery of location information

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

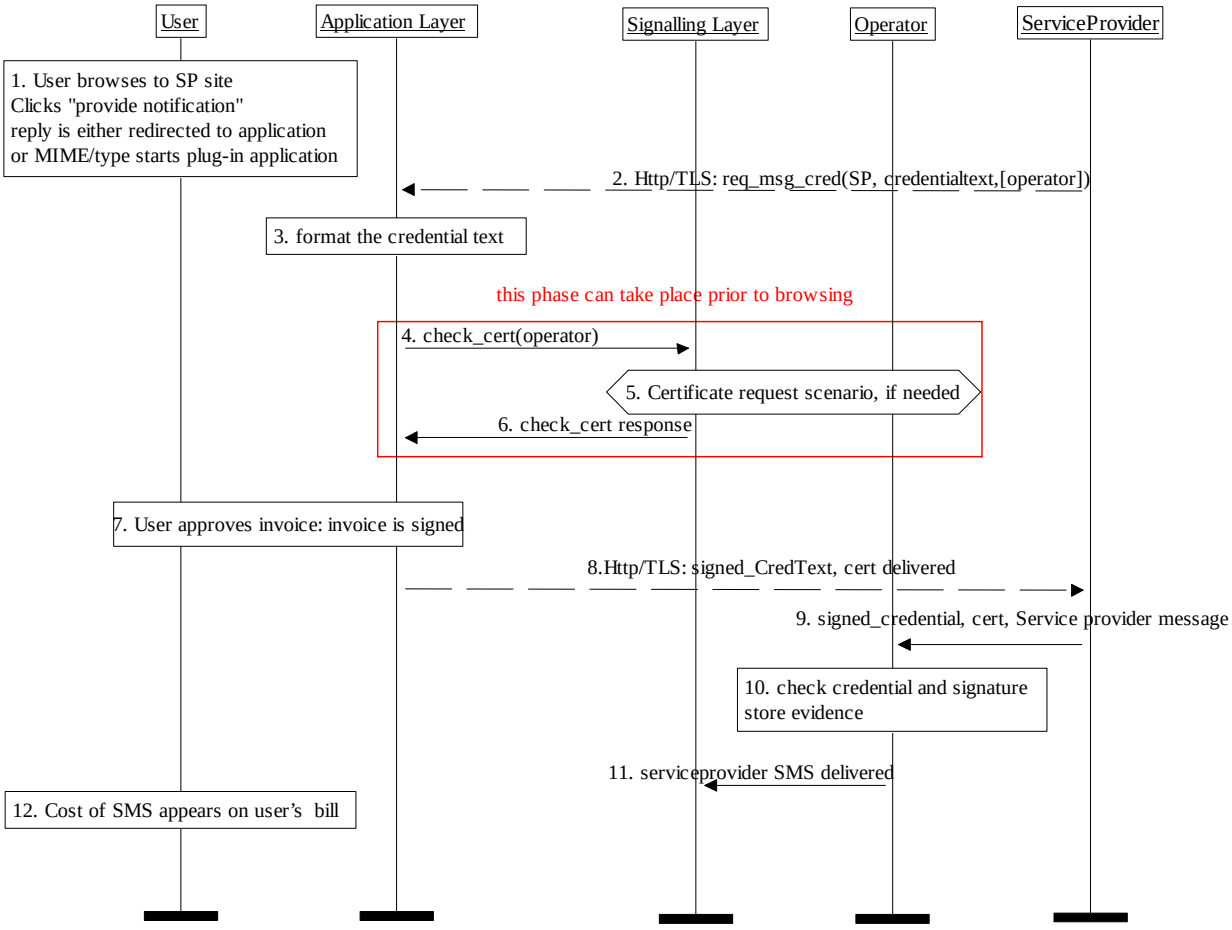

Figure 4: Delivery of notification information

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.