3GPP TSG SA WG3 Security — S3#26 **S3-020597**
19- 22 November 2002
Oxford, UK

3GPP TSG-SA WG2 Meeting #27 **Tdoc S2-023130**
Beijing, China, October 14-18, 2002.

Title: LS on subscriber certificates
Response to:
Release: Release 6
Work Item: Support for subscriber certificates

Source: SA2
To: SA3
Cc:

Contact Person:
Name: **Miikka Poikselkä**
Tel. Number: +358503210275
E-mail Address: miikka.poikselka@nokia.com

Attachments: S2-022854

---

1. Overall Description:

SA3 asked SA2's support on the selection between different architectural options for support of issuing certificates in S3-020447/ S2-022253.

SA2 discussed on subscriber certificates in SA2#27 based on S2-022854. From architectural point of view SA2 recommends a solution, which does not limit issuing of subscriber certificates and does not affect on SGSN, GGSN or CSCFs.

2. ACTIONS:

SA2 kindly request SA3 to take SA2's view into account in their further work.

3. Date of Next TSG-SA2 Meetings

SA2#28	November 11-15, 2002 (Bangkok)

3GPP TSG-SA-WG2, Meeting #27
Beijing, China, 14th - 18th October 2002

Tdoc S2-022854

Agenda Item: 9.3

Source: Nokia

Title: Architecture proposal to support subscriber certificates

Document for: Discussion and Approval

Date: 09.10.2002

---

1. Introduction

This document describes four choices for the design of architecture supporting subscriber certificates. LS from S3 (S2-022253/S3-020447) identified four choices on connecting cellular network to the Certification Authority (CA): SGSN, GGSN, IMS, and a new "gateway" type element. In this contribution we describe the architecture alternatives and functionality of elements in more detail, and discuss the pros and cons of each choice. One architecture alternative is proposed to be selected as working assumption.

2. Discussion

S1 has agreed the following requirements for subscriber certificates (3GPP TS 22.105 V6.0.0):

> For 3GPP, only the certificates issued by operators are relevant. There are two types of such certificates: subscriber certificates are issued to cellular subscribers and operator CA certificates are self-signed or issued to other operators. Issuing subscriber certificates allows operators to offer authorization and accounting of other services. Operator CA certificates obtained via a trusted channel can be used as root certificates.
>
> Operator-issued certificates in 3GPP must be such that they are compatible with other systems that allow the storage, selection, and use of certificates (e.g., WAP, LCS).
>
> The 3GPP system shall provide support for issuing certificates to the UE over the authenticated network connection. This feature shall be based on existing 3GPP system security principles and mechanisms as far as possible. The certificate management procedures must be authenticated and integrity-protected. It shall be possible to issue certificates for service usage both in the home and visited networks. It should be possible for the home operator to exercise control over service usage in the visited network.

3. Architecture alternatives

The four architecture alternatives are described in this section. The general assumption in all alternatives is that the home operator control over issuing of certificate in a visited network is needed. In three of the alternatives, home control is implemented by adding new parameters to the subscriber profile and

checking these new parameters in visited network when issuing the certificates. In the IMS based alternative the decision for issuing a certificate is done in home network, and thus also other solutions than new parameters in subscriber profile are possible.

3.1 SGSN based alternative

3.1.1 Architecture and functionalities

In this architecture alternative the CA is connected to the SGSN. The certificate issuing messages between SGSN and CA are over an IP connection. All CAs and network elements are assumed to be part of Network Domain Security (NDS), i.e. the information and the mechanisms needed for secure communication between CA and SGSN exist.

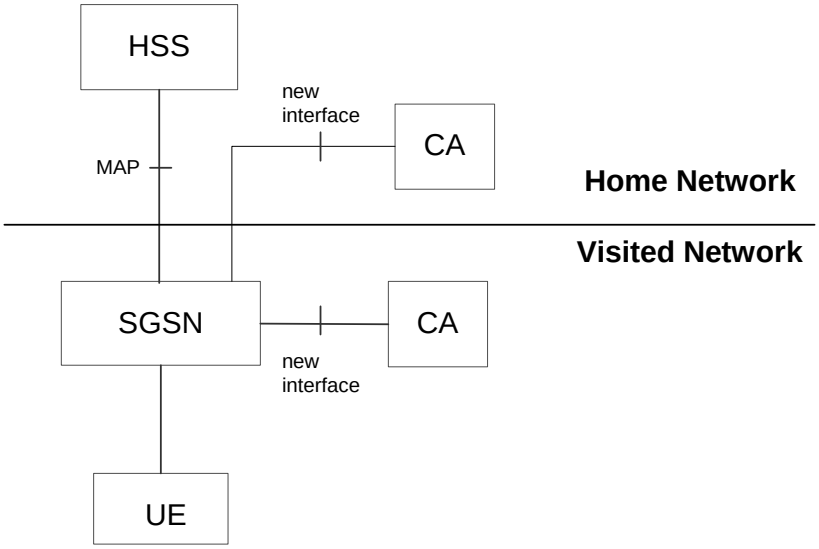

Figure 1: SGSN based network architecture to support subscriber certificates

UE sends the certificate request always to SGSN. UE indicates within the request message the network (home or visited) from which it wants the certificate.

SGSN needs to support new UE signaling and new interface to CA. SGSN shall check which type of certificate is requested (home or visited) and add needed parameters (e.g. cellular identity, certificate related parameters from subscriber profile, and the quality of authentication of subscriber) to request message before routing it to visited or home CA.

CA (or SGSN) needs to check based the subscriber data whether issuing of certificate is allowed or not.

If issuing of certificate is allowed, CA decides certificate values, generates and signs the certificate, stores record in database, and delivers the certificate back to SGSN.

3.1.2 Evaluation of the architecture

Benefits:

- Existing secure communication channel with UE used (no need to define new security procedures).
- SGSN is always located in visited network, so addressing of the local CA is easy.
- SGSN can handle easily the subscriber information check (or deliver the needed info to CA), as subscriber profile is downloaded to SGSN.

Drawbacks:

- Requires standardization of new signaling messages (in layer 3).
- New interoperator interface between the visited SGSN and the home CA is required.
- Addressing the CA in home network when user is roaming requires either that the address of the home CA is stored to the UE, or added to the subscriber profile.

3.2 GGSN based alternative

3.2.1 Architecture and functionalities

In this architecture alternative the CA is connected to the GGSN. The certificate issuing messages between GGSN and CA are over an IP connection. All CAs and network elements are assumed to be part of Network Domain Security (NDS), i.e. the information and the mechanisms needed for secure communication between CA and GGSN exist.

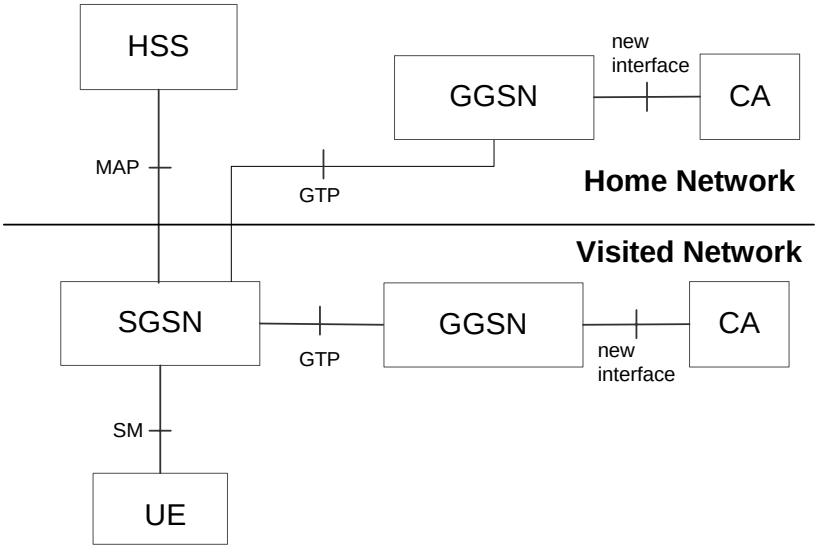

Figure 2: GGSN based network architecture to support subscriber certificates

The GGSN in the visited network is connected only with the visited CA and that the GGSN in the home network is connected only with the home CA. The UE

selects the network from which it wants the certificate and the SGSN will route the certificate request to the correct CA.

To support certificate issuing new SM messages (FFS) and GTP messages between UE and GGSN could be standardized. An alternative to new messages could be the usage of PCO IE, i.e. the certificate request could be encapsulated in the PCO IE. PCO IE is exchanged between UE and GGSN during activation, secondary activation or modification of PDP context. However, the maximum length of PCO IE is 253 bytes (TS 24.008), and since some of the subscriber certificate issuing messages are longer than 253 bytes, either user plane continuation should be used or the maximum length of PCO IE should be increased.

UE needs to support new signaling messages for certificate request procedure. UE indicates within the request message the network (home or visited) from which it wants the certificate.

SGSN needs to support new UE signaling messages, and new signaling (new messages or IEs) to deliver the needed parameters (e.g. certificate related parameters from subscriber profile, quality of authentication of subscriber) to GGSN.

GGSN needs to support new UE and SGSN signaling and new interface to CA.

CA (or GGSN) needs to check based the subscriber data whether issuing of certificate is allowed or not. If issuing of certificate is allowed, CA decides certificate values, generates and signs the certificate, stores record in database, and delivers the certificate back to GGSN.

3.2.2 Evaluation of the architecture

Benefits:

- Existing secure communication channel with UE used (no need to define new security procedures).
- GGSN is a ”natural” element from which to go to network elements that are external to PS domain.

Drawbacks:

- Standardization of new messages between UE and GGSN is required.
- Standardization of new messages or IEs between SGSN and GGSN is required to transfer subscriber parameters and quality of authentication of subscriber.
- If user has already a PDP context active to the home network, and user wants to request a certificate from the visited network, then the UE has to activate a new PRIMARY PDP context to visited network.
- The certificate issuing from visited network is coupled with other services (e.g. getting internet access) through the visited network’s GGSN, because visited GGSN can be used only if a PDP context establishment is allowed to visited network.

3.3 IMS based alternative

3.3.1 Architecture and functionalities

In this alternative the signaling between UE and CA would go through P-CSCF and S-CSCF, i.e. new interface from S-CSCF to CA would be needed. The SIP messages would be used between UE and S-CSCF.

Before certificate request is done, normal IMS registration (including P-CSCF discovery, S-CSCF selection and authentication) is done.

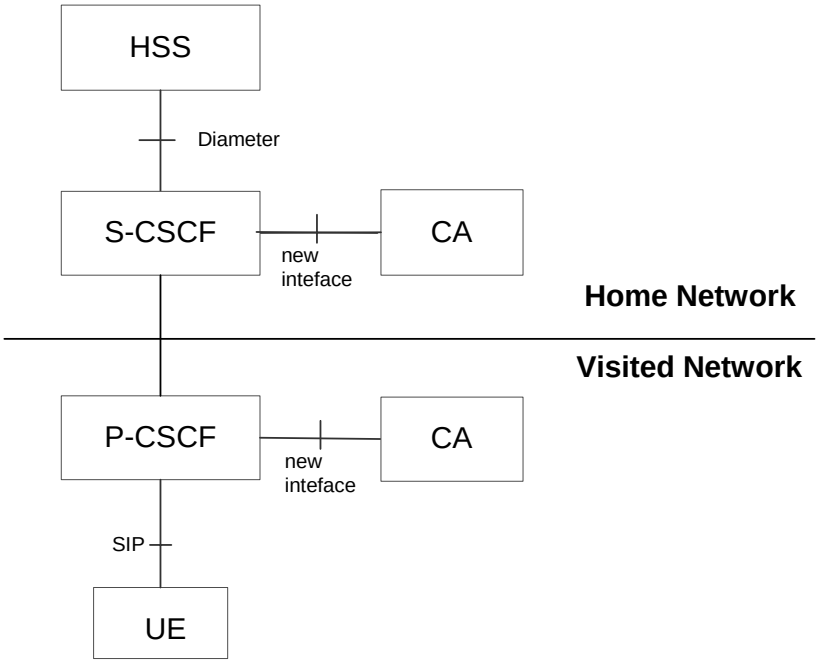

Figure 3: IMS based network architecture to support subscriber certificates

UE sends the certificate request always to S-CSCF. UE indicates within the request message the network (home or visited) from which it wants the certificate.

S-CSCF needs to check based the subscriber data whether issuing of certificate is allowed or not. If issuing of certificate is allowed, S-CSCF needs check which type of certificate is requested (home or visited), add the needed parameters (e.g. cellular identity and certificate related parameters from subscriber profile) and route the request either to home CA or back to P-CSCF (which would route it to visited CA).

If P-CSCF receives a certificate request from S-CSCF, P-CSCF needs to route it to visited CA.

CA decides certificate values, generates and signs the certificate, stores record in database, and delivers the certificate back to S-CSCF or P-CSCF.

3.3.2 Evaluation of the architecture

Benefits:

- Allows that check for issuing subscriber certificate is done always in home operator's network (added flexibility for checking parameters).
- Subscriber certificates could be obtained over any access network that provides access to IMS.

Drawbacks:

- Would make subscriber certificates, and services based on them, restricted to IMS subscribers.
- If P-CSCF is in home network, then the local CA can not be used and local services that require agreement between local operator and service provider can not be supported.
- May require IETF standardization.
- Requires changes to P-CSCF and S-CSCF.

3.4 New "Gateway" Type Element based alternative

3.4.1 Architecture and functionalities

In this alternative, a new element "Authenticator" (Au) functions as a certificate provisioning gateway for the UE. The actual authentication of the subscriber is provided by AAA server in subscribers home network.

The authentication and certificate-request procedure between UE and Au is IP-based, and hence access independent. All CAs and network elements are assumed to be part of Network Domain Security (NDS), i.e. the information and the mechanisms needed for secure communication between CA, Au and AAA server exist.

EAP AKA is a suitable candidate for building an access-independent authentication mechanism on. EAP AKA is currently an IETF draft and will be used also for authenticating a subscriber accessing 3GPP WLAN Subsystem. EAP/AKA provides means to exchange AKA authentication messages encapsulated within the extensible authentication protocol (EAP). EAP is increasingly widely supported in routers, network access points, and end user PCs. If EAP AKA is chosen, then the UE platform must include an EAP AKA implementation.

If EAP AKA is the authentication mechanism, a natural choice for transporting certificate request/response messages is PIC (A pre-IKE credential provisioning protocol) being developed by the IETF ipsra working group. PIC is currently also an IETF draft, in last call. PIC can be run between any two IP-capable entities connected to the same internetwork. It first sets up a server-authenticated encrypted connection between the client and the server and then sends any EAP payload through this connection.

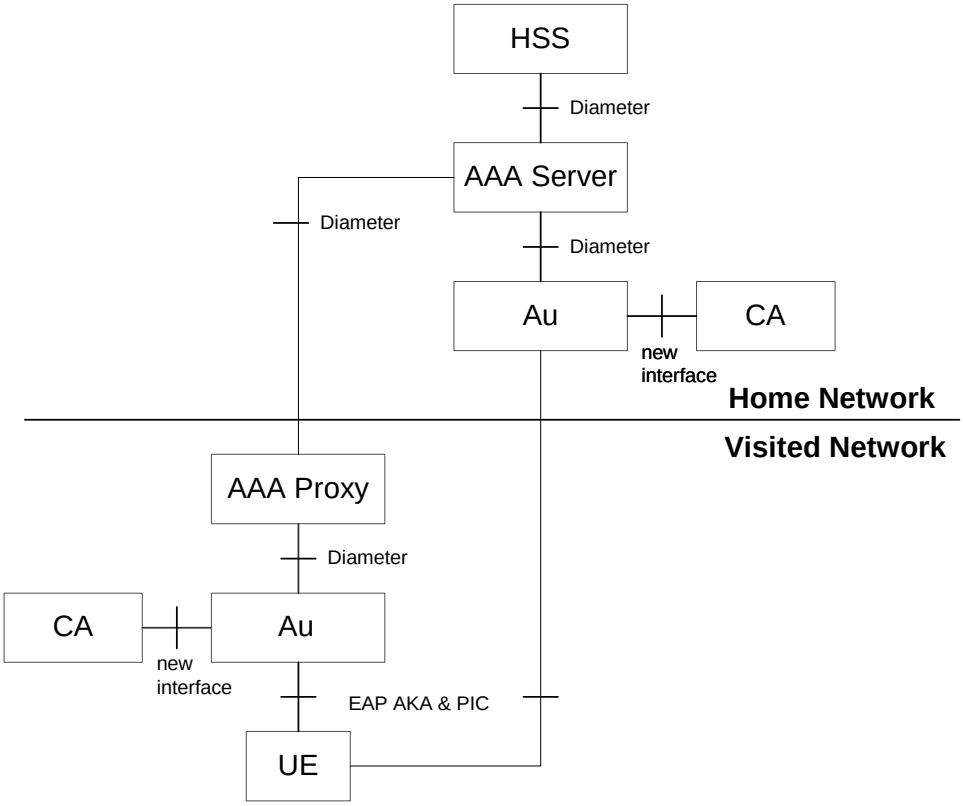

Figure 4: New element based network architecture to support subscriber certificates

UE first locates the right authenticator (visited or home), and sends a certificate request to it using PIC and EAP AKA. The authenticator will route the EAP messages to an AAA server in subscribers home network, potentially using an AAA proxy in its own network. The AAA server will reply to the authenticator indicating the success/failure of the AKA authentication, as well as including any needed subscriber information retrieved from HSS. If necessary, a MAP-based interface can be used as an interim measure between the AAA Proxy and the HSS.

Before issuing a certificate, the CA, the authenticator or the AAA server needs to check based on the subscriber data whether issuing of certificate is allowed or not.

After successful authentication and authorization, CA decides certificate values, generates and signs the certificate, stores record in database, and delivers the certificate back to the authenticator which then forwards it to the UE via the authenticated encrypted PIC connection.

Terminal must support the new authentication mechanism (e.g., PIC, EAP, and EAP AKA).

Authenticator needs access to subscriber information stored in HSS: either directly, using the MAP-based roaming infrastructure, or indirectly, using a DIAMETER-based roaming infrastructure.

3.4.2 Evaluation of the architecture

Benefits:

- Access independence for certificate requests
- Technically feasible
- Possible to deploy over existing PS domain implementations
- No arbitrary constraints: anything can be specified and designed in a new element
- Synergies with WLAN interworking security solutions possible
- Changes to application layer easier to build on top of legacy terminals (supporting e.g. WIM and USIM)

Drawbacks:

- Terminals have to support PIC, EAP, and EAP AKA
    - Alternative: HTTP Digest AKA and IPsec, but additional protocol messages needed
- How does UE find the authenticator? (when certificates are issued by visited networks)
    - It should be done similar to the way in which P-CSCF discovery is done in IMS. I.e., UE can be informed of the address of the authenticator using DHCP and DNS, or during PDP context establishment/update.
    - Service Location Protocol can be used; but then network and terminal should support SLP
    - In all of the above, when connected via PS domain, the UE shall open a PDP context to the local GGSN in order to find the address of the local authenticator.
- A new independent domain that consumes authentication vectors is needed unless WLAN subsystem can be reused for executing the subscribers authentication
- Home operator control over certificate issuing requires new attributes in subscriber profile and retrieval of subscriber profile to a new element has to be arranged

4. Proposal

The new element based architecture is proposed to be selected as working assumption for supporting subscriber certificates, because it supports access independence and offers most flexibility. It also avoids changes cellular protocols and changes to existing PS domain network elements.