**3GPP TSG SA WG3 Security — S3#26** **S3-020634**
**19- 22 November 2002**
**Oxford, UK**

**Source:** Nokia

**Title:** Architecture to support subscriber certificates based on new "gateway" type element

**Document for:** Discussion and Approval

**Agenda Item:** 7.7

---

## 1 Background

SA3 identified four architecture alternatives for supporting subscriber certificates: SGSN, GGSN, IMS and new "gateway" type element based architectures. In Helsinki plenary meeting #24, SA3 asked SA2's support on the architecture selection.

SA2 gave the following recommendation for the architecture selection (Tdoc S3-020597, i.e.,S2-023130):

> *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 Introduction

This document describes the new "gateway" type element based architecture supporting subscriber certificates. Also signalling flow is proposed and open issues are identified.

Home control has been identified as an important requirement for subscriber certificates in SA1, SA2 and SA3 discussions. In this contribution it is proposed that the home control is implemented by adding new parameters to the subscriber profile in HLR/HSS and checking these new parameters in the visited network when issuing the certificates.

## 3 New "gateway" type element solution

### 3.1 Architecture

In this architecture, a new element "Authenticator" (Au) functions as a certificate provisioning gateway for the UE. The actual authentication of the subscriber is provided by the AAA server in subscriber's 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 covered by Network Domain Security (NDS), i.e. the information

and the mechanisms needed for secure communication between CA, Au and AAA server exist.

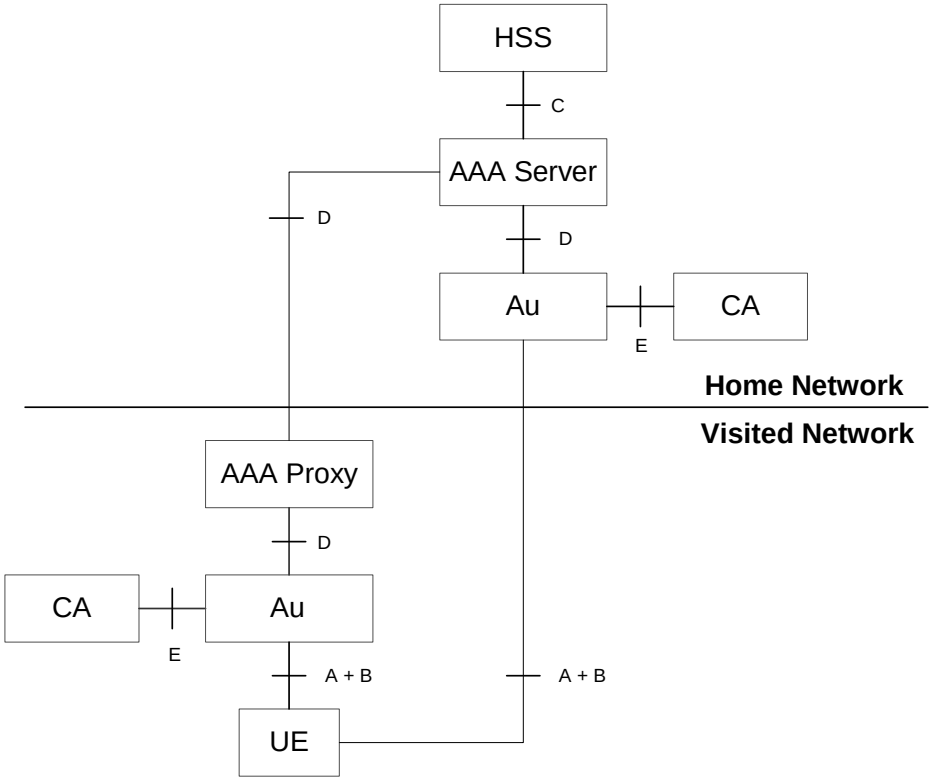


Figure 1: New element based network architecture to support subscriber certificates

User authentication for certification requests shall be based on a cellular subscription. Therefore the underlying authentication protocol shall be AKA.

In Figure 1, the A protocol is a suitable encapsulation for AKA that allows it to be carried out over IP networks; it could be EAP AKA or HTTP Digest AKA.

Protocol B uses the security association resulting from protocol A to protect request and delivery of the certificates, it could be based e.g. on IPsec.

Protocol C is the protocol used between AAA Server and HSS. It could be e.g. DIAMETER or MAP.

Protocol D is the protocol used between $Au_H$ and AAA Server, between $Au_V$ and AAA Proxy, and between AAA Proxy and AAA Server. It could be e.g. DIAMETER.

Protocol E is the protocol used between CA and $Au_H$ or $Au_V$ to protect the request and delivery of the certificates. It could be based on NDS protection.

### 3.2 Functionalities of the elements

AAA server is responsible for authenticating the user's identity with the AKA protocol. AAA Server will also relay the needed subscriber information retrieved from HSS to AAA proxy or Au.

In case of roaming, AAA proxy in the visited network fetches authentication data through AAA server in the home network.

The authenticator Au functions as a certificate provisioning gateway for the UE. Au checks user's request against the subscriber's data to decide whether issuing of certificate is allowed.

CA decides values in the certificate, generates and signs the certificate, and stores the record into the database.

Terminal must support the new authentication mechanism. The address of home Au maybe discovered or stored in the UE. The address of visited Au must be discovered.

## 3.3 Proposed signalling flows

### 3.3.1 Certificate issuing by the home network CA

Figure 2 depicts the proposed signalling flow in the case where the subscriber certificate is issued by the home network.

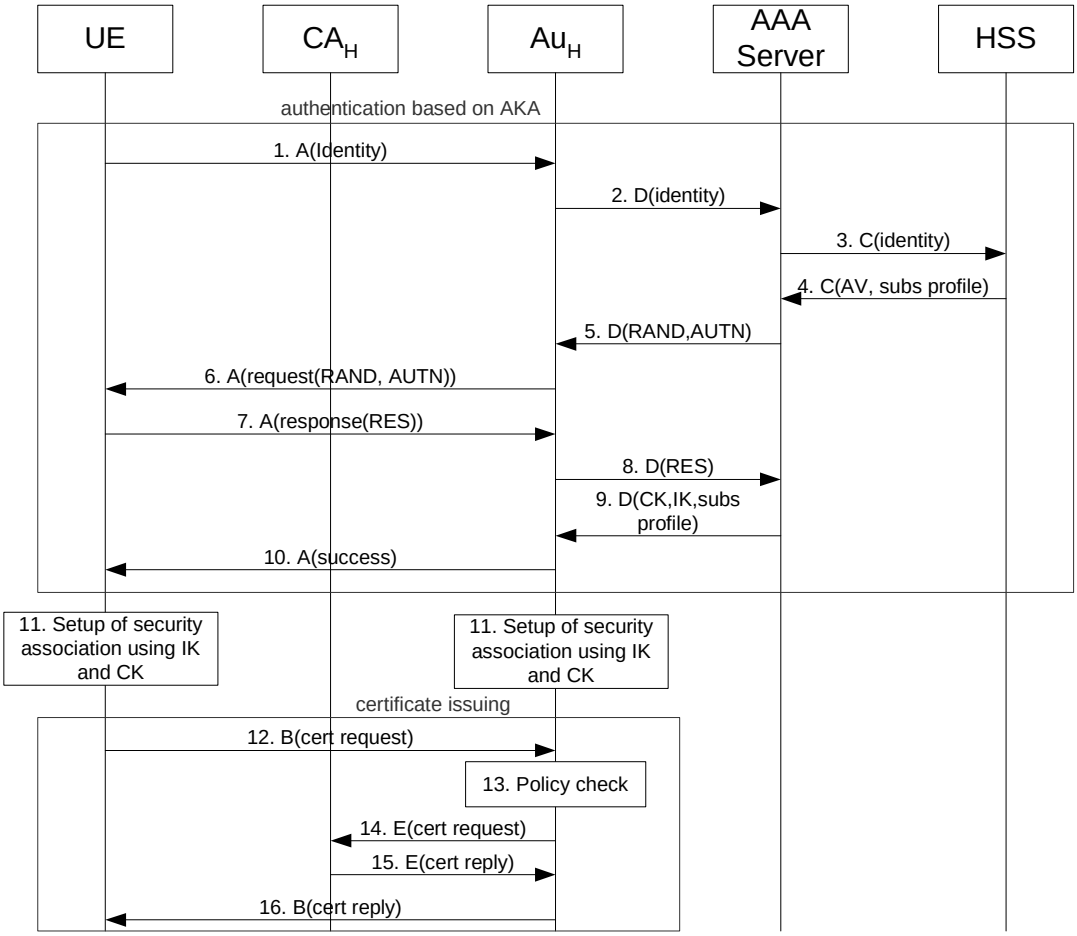


Figure 2: Certificate issuing by the home network CA

1. UE sends a message with subscriber's identity to the home Authenticator ($Au_H$).

2. $Au_H$ forwards the message to AAA Server.

3. AAA Server requests the subscriber profile data related to certificates and Authentication Vector(s) (AV) from HSS.

4. HSS sends the requested subscriber profile data related to certificates and AV(s) to AAA Server.

5. AAA Server sends request message with RAND and AUTN attributes to $Au_H$.

6. $Au_H$ forwards the challenge request message to UE.

7. UE computes the CK, IK and RES and sends RES to $Au_H$.

8. $Au_H$ forwards the message containing the RES to AAA Server.

9. AAA Server verifies the RES. If the verification is successful AAA Server sends Success message, CK and IK, and necessary subscriber profile data related to certificates to $Au_H$.

10. $Au_H$ sends the Success message to UE and stores the necessary subscriber profile data related to certificates.

11. UE and $Au_H$ setup security association using IK and CK.

12. After the security association setup is done, UE sends a certificate request to $Au_H$ (e.g., PKCS#10 CertificateRequest).

13. $Au_H$ checks the subscriber profile data related to certificates and other policy data if the certificate issuing is allowed. If the request is for an operator CA certificate, the next two steps are omitted: $Au_H$ retrieves the certificate from its storage and returns it to UE.

14. If it is allowed, $Au_H$ forwards the certification request to home certification authority ($CA_H$).

15. $CA_H$ verifies the request, generates subscriber certificate, signs it, and sends the subscriber certificate or subscriber certificate URL back to $Au_H$.

16. $Au_H$ sends certificate or certificate URL to UE.

### 3.3.2 Certificate issuing by the visited network CA

Figure 3 depicts the proposed signalling flow in the case where the subscriber certificate is issued by the visited network and UE uses visited Authenticator.

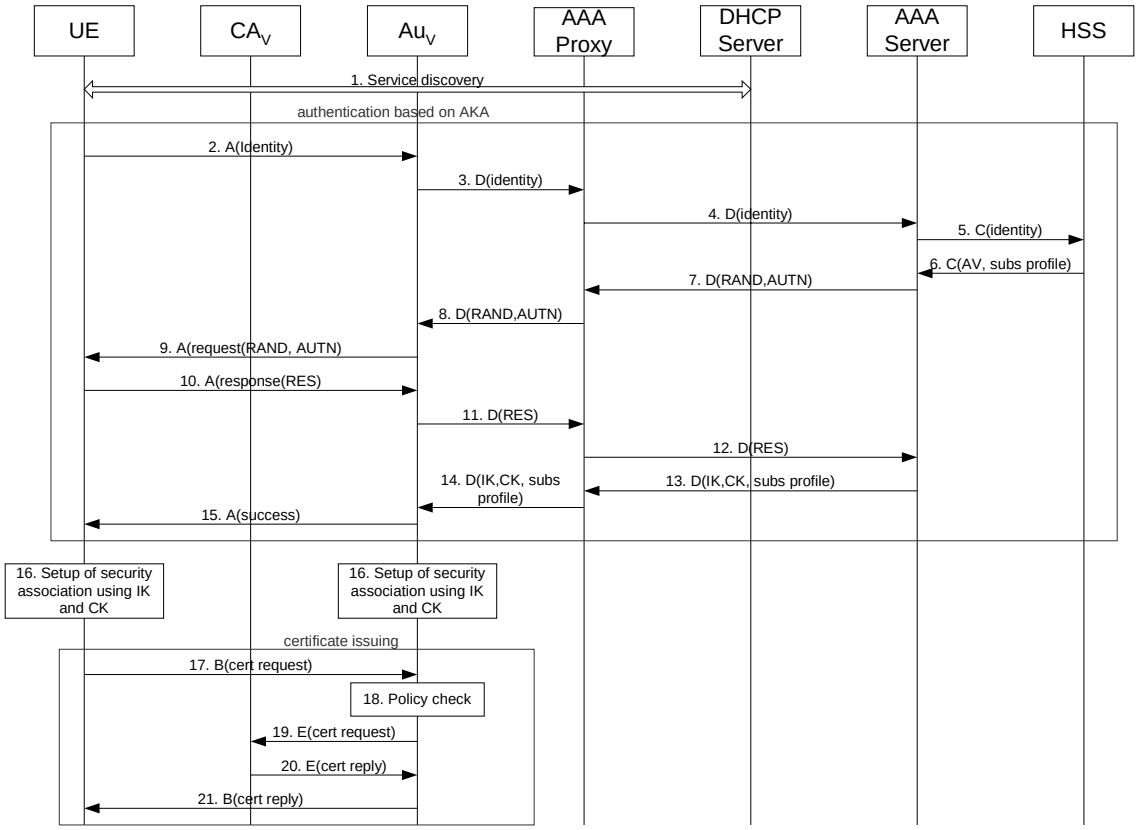


Figure 3: Certificate issuing by the visited network CA

1. Service discovery is done (e.g. DHCP may be used) by UE to learn the address of $Au_V$.
2. UE sends a message with subscriber's identity to $Au_V$.
3. $Au_V$ forwards the message to AAA Proxy
4. AAA Proxy in turn forwards the message to AAA Server.
5. AAA Server requests the subscriber profile data related to certificates and AV(s) from HSS.
6. HSS sends the subscriber profile data related to certificates and AV(s) to AAA Server.
7. AAA Server sends a message with RAND and AUTN parameters to AAA Proxy.
8. AAA Proxy sends the message with RAND and AUTN attributes to $Au_V$.
9. $Au_V$ sends the challenge request message to UE.
10. UE computes the CK, IK and RES and sends RES to $Au_V$.
11. $Au_V$ sends the response message to AAA Proxy.
12. AAA Proxy forwards response message to AAA Server.

13. AAA Server verifies the RES. If the verification is successful AAA Server send success message, IK and CK, and necessary subscriber profile data related to certificates to the AAA Proxy.

14. AAA Proxy sends the success message, IK and CK, and necessary subscriber profile data related to certificates to $Au_V$.

15. $Au_V$ sends the Success message to UE and stores subscriber profile data related to certificates locally.

16. UE and $Au_V$ setup security association using IK and CK.

17. After the security association is done, UE sends a certificate request to $Au_V$ (e.g., PKCS#10 CertificateRequest).

18. $Au_V$ checks the subscriber profile data related to certificates and other policy data if the certificate issuing is allowed. If the request is for an operator CA certificate, the next two steps are omitted: $Au_V$ retrieves the certificate from its storage and returns it to UE.

19. If it is allowed, $Au_V$ forwards the certification request to $CA_V$.

20. $CA_V$ verifies the request, generates subscriber's certificate, signs it, and sends the subscriber certificate or subscriber certificate URL back to $Au_V$.

21. $Au_V$ sends the certificate or certificate URL to UE.

### 3.4 Open issues

The open issues are listed in this section. The selected solution may affect the signaling flows described in clause 3.3.

User authentication protocol is to be selected from below:

- EAP AKA over UDP or TCP,
- EAP AKA over PIC, or
- HTTP Digest AKA.

How to bind certification request/response to subscriber authentication:

- IPSec SA (Security Association) based on IK and CK,
- Use IK to authenticate existing secure channel (e.g. PIC), or
- Use IK and CK to create some other secure channel (e.g., TLS).

Certification request syntax:

- PKCS#10,
- PKIX CRMF (certificate request message format), or
- New syntax defined by 3GPP.

Certificate format:

- WAP Certificate and CRL Profiles (WAP-211-WAPCert)
- New certificate and CRL profiles defined by 3GPP

How does the UE find the authenticator when the address of Au is not stored to UE? This is needed in the visited network case and possibly also in the home network case.

- It could 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.
- 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.

Sequence number handling:

- A new independent domain that consumes authentication vectors is needed unless enough synergies are found with some of the existing domains (e.g. WLAN subsystem) to justify common sequence numbers.

What is the new data that needs to be added to subscriber profile to support home operator control. E.g. the profile could contain indication whether the subscriber can use his signing key in authentication and/or in authorization and accounting.

## 4 Proposal

We propose the SA3 plenary meeting #26:

- to endorse the SA2 recommendation about the endpoint of certificate request, i.e. the endpoint is not existing element in PS domain or in IMS.
- to create new TS for Stage 2 description of subscriber certificates.
- to use the architecture and signalling flows presented in this document as basis for creating the new TS.