3GPP TSG SA WG3 Security — S3#26 **S3-020677**
19- 22 November 2002
Oxford, UK

Agenda Item: 7.7

Source: Alcatel

Title: Alternative proposals for subscriber certificate supporting architecture

Document for: Discussion

Introduction

There are a number of problems envisaged with the current Nokia proposal contained in S2-022854.

The current Nokia proposal for a new “gateway” type element is proposing an EAP AKA authentication step specifically as part of the certificate request procedure. This extraneous authentication step seems to be redundant given that the UE would already have been authenticated for access to the network, either via the SGSN or via the P-CSCF. Does this mean a new “domain” for AKA in addition to GPRS and UMTS?

The UE should be able to rely on the previous authentication step, which already gives the UE secure GPRS signalling access to the SGSN, or secure IMS access to the P-CSCF. This reason leads us to back a simple solution where the secure link between UE and SGSN could be reused for a request to the CA. The drawback here is that the SGSN and UE would require new signalling messages to perform this task, but this is not necessarily a forbidding reason.

In fact, the existing S1 requirements for subscriber certificate requests leave some room for ambiguity. This contribution suggests some clarifications of the requirements.

Also, the current Nokia proposal for a new “gateway” type element proposes the use of PIC as a protocol to request and deliver subscriber certificates. The use of PIC is not a suitable choice of protocol for this purpose due to the lack of current and future implementations of this protocol. Since we are trying to solve the issue of certificate requests and management, perhaps usage of protocols specialised for this task could be employed, for example CMP/CRMF as defined in RFC’s 2510 and 2511.

The complete use of PIC, EAP, and EAP AKA in the current Nokia proposal is unclear as neither detailled call flows nor a detailled description of the process involved is provided.

This contribution suggests alternative solutions as as further described below, after we suggest some clarifications of the general requirements.

Clarification of requirements

Following is a suggested clarification of the requirements from S1 for the requesting of subscriber certificates.

A] In order for the UE to access local services in a visited network, the visited network should be able to issue certificates. In this case, certificates are issued to the UE based on subscriber information retrieved from the home network.

B] The home network shall have control on whether or not the visited network may issue certificates to a UE in the visited network.

C] The manner in which the UE receives the certificates should be access, as well as service, independent. (Note: this would then exclude the first 3 alternatives in the Nokia proposal as described in S2-022854).

D] The way to ensure the user is authenticated to the network before the issuing of certificates could be access dependent.

E] It shall be possible to issue certificates to users equipped with a USIM or SIM.

F] The certificate request is carried over the data plane.

Alternative solutions

1] Using Diameter with separate authenticator and CA

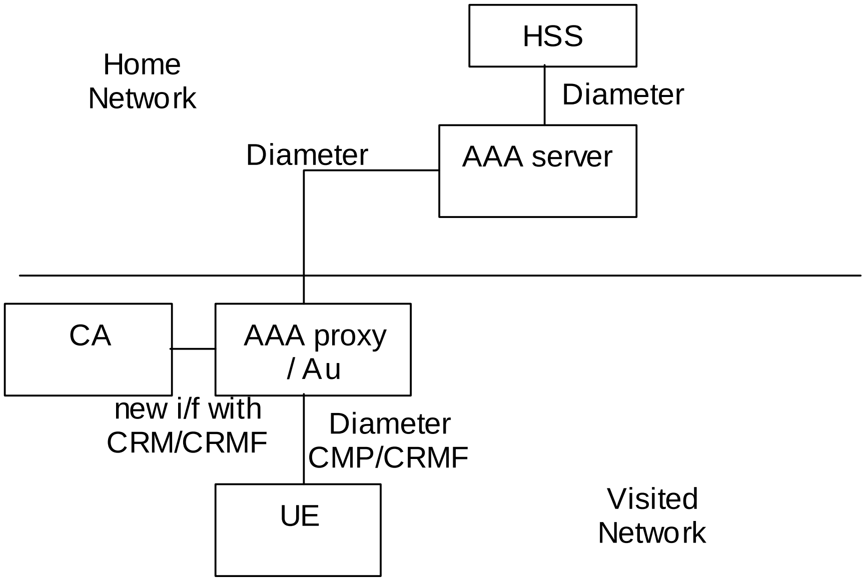
In the first of the alternative solutions, a Diameter client can be positioned in the UE. There is a first step performing authentication of the UE for the purposes of authenticated certificate requests, and the second step of the certificate request itself.

The first step involves the UE performing authentication via Diameter with EAP/AKA to the authenticator network element. This authenticator will play the role of an AAA proxy in the visited network, or an AAA server in the home network. During this phase, the EAP/AKA process must clearly indicate to the home network that his authentication phase is for certification request reasons only.

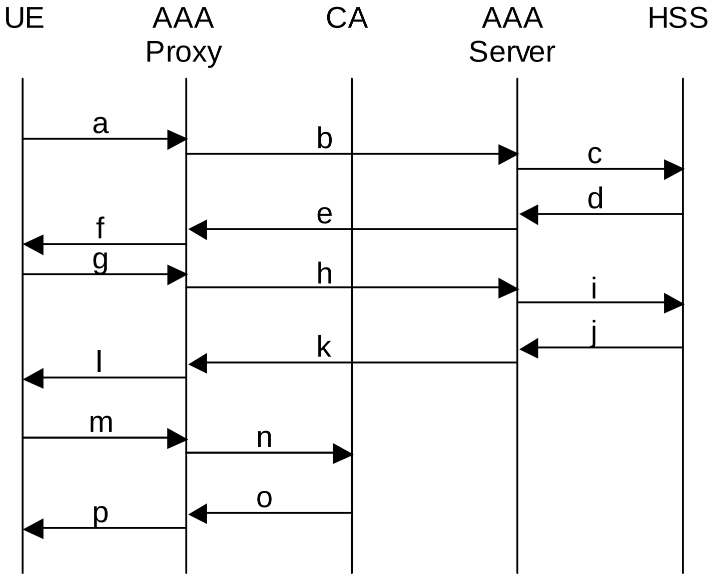
The second step involves the UE sending CMP/CRMF certificate requests to the authenticator network element, who will interact with the CA over a new interface passing the CMP/CRMF messages to it.

Security of the certificate request message and the associated response between the UE and the CA relies both on the hop-by-hop security provided by the underlying network architecture (e.g. providing confidentiality) and on the end-to-end auth/integrity mechanism integrated into CRMF/CMP.

The associated architecture for a UE in a visited network is depicted in the diagram below.



Following is a scenario depicting the authentication phase (a to l), and the certificate request phase (m to p), for a UE in a visited network.



Scenario description:

a: Diameter request for certificate request authentication.

b: Diameter request for certificate request authentication.

c: Diameter request for certificate request authentication vectors.

d: Diameter answer with authentication vectors.

e: Diameter answer with AKA authentication challenge.

f: Diameter answer with AKA authentication challenge.

g: Diameter request with AKA authentication challenge response.

h: Diameter request with AKA authentication challenge response.

i: (Optional) Diameter request with database update.

j: (Optional) Diameter answer with database update acknowledge.

k: Diameter answer with authentication acknowledge.

l: Diameter answer with authentication acknowledge.

m: CMP pkiMsg containing CRMF CertReqMsg.

n: CMP pkiMsg containing CRMF CertReqMsg.

o: CMP finalMsgRep containing certificate.

p: CMP finalMsgRep containing certificate.

2] Using Diameter with combined authenticator and CA

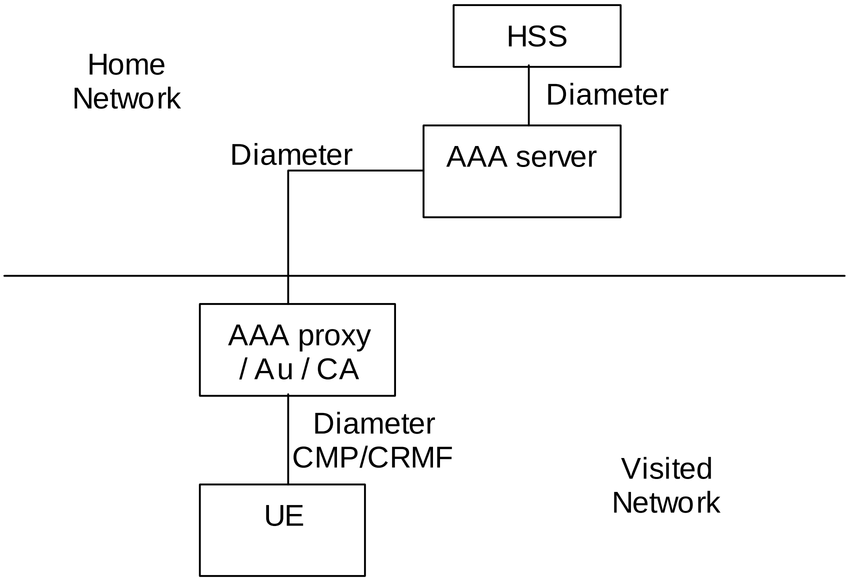
A second alternative solution would be to have a combined authenticator network element and CA. The solution would work in a similar way as to the first alternative solution described above. With a Diameter client positioned in the UE, there is a first step performing authentication of the UE for the purposes of authenticated certificate requests, and the second step of the certificate request itself.

The first step is identical to the first alternative described above.

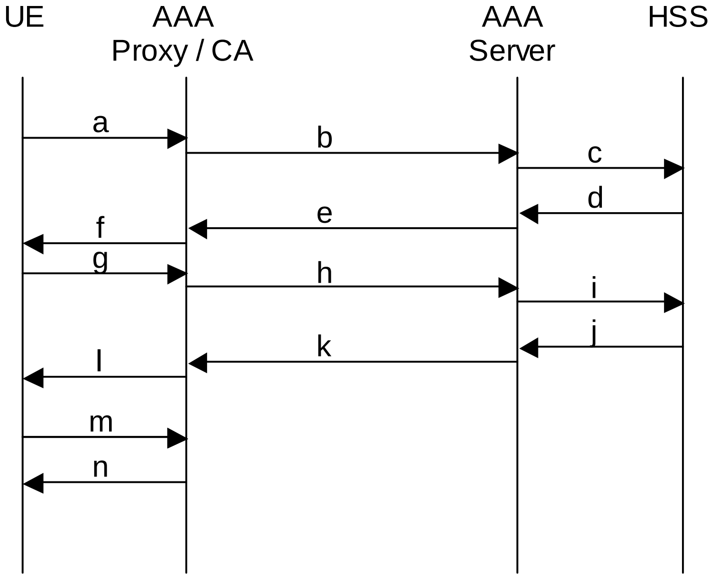
The second step involves the UE sending CMP/CRMF certificate requests to the authenticator network element which is also the CA.

Security of the certificate request message and the associated response between the UE and the CA relies both on the hop-by-hop security provided by the underlying network architecture (e.g. providing confidentiality) and on the end-to-end auth/integrity mechanism integrated into CRMF/CMP.

The associated architecture for a UE in a visited network is depicted in the diagram below.



Following is a scenario depicting the authentication phase (a to l), and the certificate request phase (m to n), for a UE in a visited network.



Scenario description:

a: Diameter request for certificate request authentication.

b: Diameter request for certificate request authentication.

c: Diameter request for certificate request authentication vectors.

d: Diameter answer with authentication vectors.

e: Diameter answer with AKA authentication challenge.

f: Diameter answer with AKA authentication challenge.

g: Diameter request with AKA authentication challenge response.

h: Diameter request with AKA authentication challenge response.

i: (Optional) Diameter request with database update.

j: (Optional) Diameter answer with database update acknowledge.

k: Diameter answer with authentication acknowledge.

l: Diameter answer with authentication acknowledge.

m: CMP pkiMsg containing CRMF CertReqMsg.

n: CMP finalMsgRep containing certificate.

3] Pre-loaded long lasting public/private keys

An alternative solution could be to issue the UE with a pre-loaded, long lasting, public/private key pair from the home network. The UE can issue a request for a certificate to the CA, signing the request with the long lasting private key.

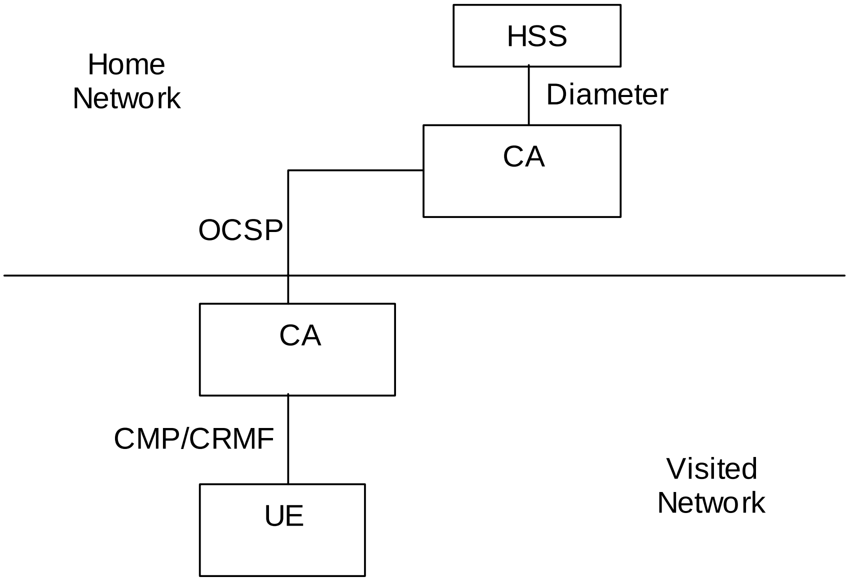
The underlying network secure link between UE and SGSN is relied upon to provide integrity protection and confidentiality for the UE to CA link.

There is no need for a separate authenticator network element in this solution. There is also no need for a separate AKA procedure to be executed.

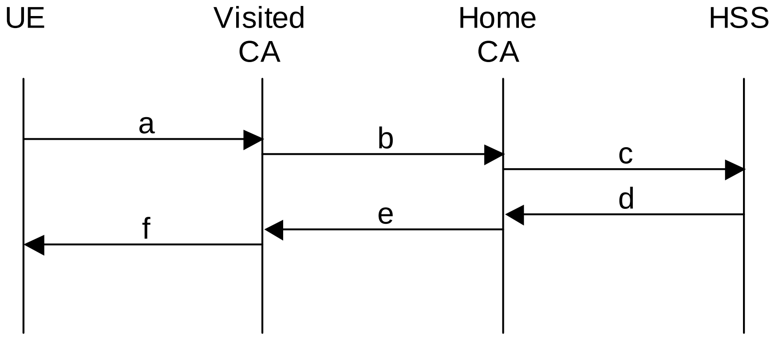
Validation of the UE's signature in the certificate request message can be performed in the visited network provided there is an inter-operator PKI infrastructure, or in the home network using a certificate validation protocol, e.g. OCSP.

The fact that a long lasting public/private key pair is used does not require interaction of the HSS to validate the certificate request, but may be utilised as an option to provide control over the key pair.

The associated architecture for a UE in a visited network is depicted in the diagram below.



Following is a scenario depicting the certificate request phase (a and f), and the UE's request certificate validation phase (b and e), for a UE in a visited network.



Scenario description:

a: CMP pkiMsg containing CRMF CertReqMsg.

b: OCSPRequest sent to Home CA to validate UE's certificate.

c: (Optional) Diameter request for subscriber related key information from HSS.

d: (Optional) Diameter answer with subscriber related key information.

e: OCSPResponse containing UE's request certificate validation response.

f: CMP finalMsgRep containing certificate.

4] Re-use of SGSN

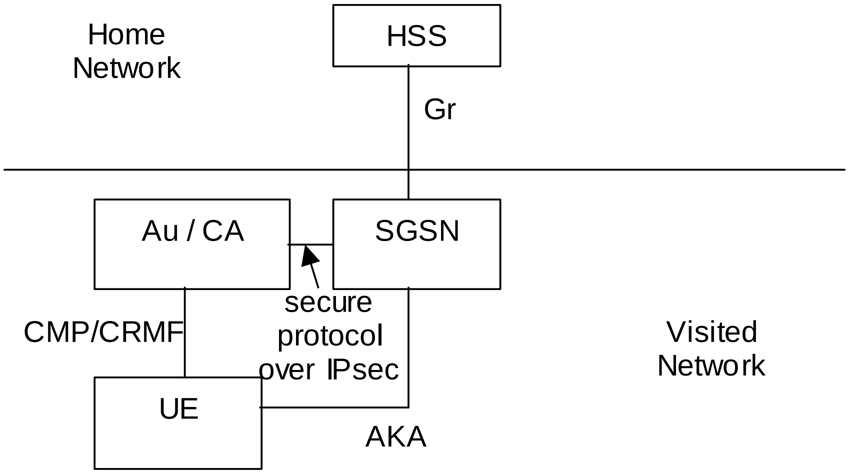
Another alternative solution is to assume that the authenticator network element already has a copy of the shared key from the initial UMTS or IMS AKA procedure, as well as subscriber data downloaded from the HSS pertaining to certificate requests. Such a solution requires a secure way of transporting the keying material (IK/CK) and relevant subscriber information from the SGSN or P-CSCF to the authenticator network element. This security could be provided as per NDS/IP and use of IPsec, but the protocol itself to transport the shared key and subscriber information is to be decided.

Security of the certificate request message and the associated response between the UE and the CA relies both on the hop-by-hop security provided by the underlying network architecture (e.g. providing confidentiality) and on the end-to-end auth/integrity mechanism integrated into CRMF/CMP.

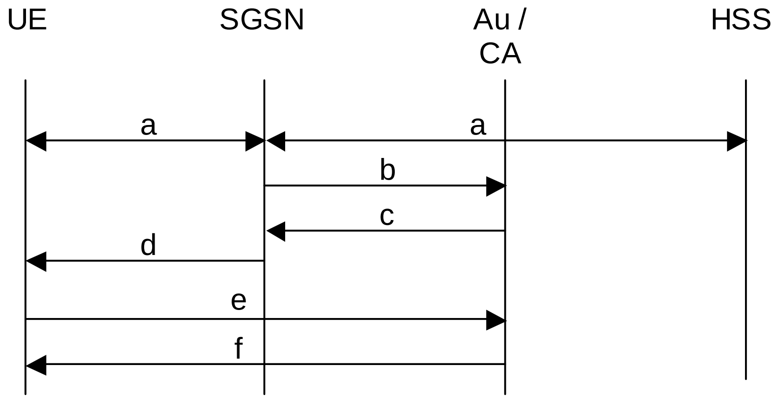
Such a solution would not conform to SA2's request (via LS S2-023130 from SA2#27 in Beijing) that the GSNs and CSCFs not be affected, but would result in a simple solution to the problem. This solution is also viable if suggestion D] for the clarification of requirements is agreed to, namely that the way to ensure the user is authenticated to the network before the issuing of certificates could be access dependent. In addition, this solution does not require a dedicated AKA domain for certificate request authentication (as is needed in the last Nokia alternative in S2-022854).

When the authenticator network element has the shared key, the UE can then issue certificate request messages to it (to be relayed to the CA) in a similar fashion as in solutions 1] and 2] above.

The associated architecture for a UE in a visited network is depicted in the diagram below.



Following is a scenario depicting the normal AKA procedure and information distribution phase (a to d), and the certificate request phase (e and f) for a UE in a visited network.



Scenario description:

a: Normal UMTS AKA procedure, with download of AKA vectors and subscriber data from the HSS.

b: Sending of shared secret key and relevant subscriber data via secure link to Au/CA.

c: Acknowledge of receipt.

d: (Optional) Acknowledge / indication to UE that Au/CA has received the information.

e: CMP pkiMsg containing CRMF CertReqMsg.

f: CMP finalMsgRep containing certificate.

Note: Step "d" is optional. This would require an impact in the UE to support this, but without it, there is the possibility that the UE would initiate a certificate request "e" before the Au/CA has the necessary data from "b".

Proposal

With respect to the current Nokia proposal contained in S2-022854 that proposes a new "gateway" type element and which is proposing EAP AKA and PIC for the authentication and certificate request procedure, different proposals should be considered. Namely, whether a separate authentication step is needed at all, and that alternative protocols are more suited to the certificate request and management procedure, as well as for the secondary authentication if needed.

A clarification to the requirements for subscriber certificate requests is also provided for further consideration.