3GPP TSG SA WG3 Security — S3#24 **S3-020377**

9 - 12 July 2002

Helsinki, Finland

Source: **Nokia**

Title: **Architecture alternatives for supporting subscriber certificates**

Document for: **Discussion**

Agenda Item: **7.7**

1. Introduction

This contribution presents some identified requirements for architecture supporting the issuing of subscriber certificates, and four different architecture alternatives.

2. Architecture requirements

The following requirements for architecture selection have been identified.

- Integrity protected channel between UE and network (CA) is required.
- Needs to support CA in visited network.
  - This is needed as service providers will typically have relationship only to the local operators in the same geographic region. Without a global PKI they cannot recognize certificates issued by the home network.
- Needs to support CA in home network.
  - Some services (e.g. home network based services or LCS) may require certificates from home network.
- Access independent solution would be ideal.

3. Architecture alternatives

In this section different architecture alternatives and their benefits and drawbacks are described.

CA connected to SGSN

In this alternative the signaling between UE and CA would go through SGSN, i.e. new interface from SGSN to CA would be needed. The signaling messages between UE and SGSN would be defined in 3GPP TS 24.008.

Benefits:

- integrity protected channel between UE and RNC can be utilized,
- SGSN is located always in the visited network, so it supports easily CA in the visited network, and
- SGSN can handle subscriber information.

Drawbacks:

- addressing CA in home network when user is roaming needs specific mechanism
- requires CA interface in SGSN, and
- this solution is not access independent.

CA connected to GGSN

In this alternative the signaling between UE and CA would go through GGSN, i.e. new interface from GGSN to CA would be needed. Benefits:

- GGSN is a natural entity to support this, as GGSN provides access to all services, and
- integrity protected channel between UE and RNC could be utilized.

Drawbacks:

- requires CA interface in GGSN,
- GGSN does not have access to all subscriber information,
- UE - GGSN signaling might have some limitations, and
- this solution is not access independent.

IMS based (CA connected to S-CSCF)

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, and possibly also to CA.

One example of possible message flow is presented here:

1. UE indicates whether it wants certificate from home or visited network.
2. P-CSCF (in visited network) will include to request message the address of local CA.
3. S-CSCF could check that issuing certificate is allowed.
4. S-CSCF would check request type, and divert request either to home or visited CA.

Benefits:

- does not require changes to SGSN or GGSN, and

- subscriber certificates could be obtained over any access network that provides access to IMS.

Drawbacks:

- would make subscriber certificates, and services based on them, dependent on IMS deployment,
- may require IETF standardization,
- terminating certificate request to visited network might be problematic, and
- if P-CSCF is in home network, then local CA can not be used and local services that require agreement between local operator and service provider can not be supported.

CA connected to New Element

In this alternative the signaling between UE and CA would go through a new element, i.e. this new element would need an interface to CA. The signaling between UE and this element would happen over normal PDP context. The used protocol could be e.g. HTTP/AKA.

Benefits:

- does not require changes to SGSN or GGSN,
- this solution may be built to be access independent.

Drawbacks:

- requires new element,
- addional authentication between new element and UE needs to be done,
- new element requires access to subscriber information (in addition to CA interface),

.

4. Conclusions

The SGSN based architecture was preferred earlier, as it supports the integrity protected channel most naturally. However, also other alternatives can be considered.