3GPP TSG SA WG3 Security — S3#24 **S3-020378**

9 - 12 July 2002

Helsinki, Finland

Source: **Nokia**

Title: **Security and other requirements for subscriber certificates**

Document for: **Discussion and decision**

Agenda Item: **7.7**

1. Introduction

There exists a need for a global scale authorization infrastructure for various applications and services. This may be based on the 3GPP system security architecture. Many of the~~se~~ emerging services will be provided by parties that are not necessarily trusted by the cellular operators nor by cellular subscribers. Therefore technical means to deal with, and preferably minimize, disputes between subscribers and service providers is necessary. Authorization of such services may be based on credentials like digital signatures. The service provider shall use subscriber certificates in verifying credentials. The UE may also use certificates of operators (operator certificates) and other certificates issued by operators in verifying credentials supplied by service providers.

The purpose of Subscriber Certificates WI is to use global and secure authorization and charging infrastructure of mobile networks to support local architecture for digital signatures. [WID]

2. Security requirements

The following security requirements for subscriber and operator certificates have been identified:

- The certificate request/response messages must be authenticated and integrity-protected so that
  - the CA can verify that a request originated from (the UE of) a specific cellular subscriber; this is mandatory in the case of a request for a subscriber certificate.
  - the UE can verify that the response originated from a legitimate cellular network element; this is mandatory in the case of the response to a request for an operator certificate.
  - a recipient can be confident that a potential attacker could not have modified a received message.
- The mechanisms to secure the certificate request/response messages leverage the 3GPP system security infrastructure.

3. Other requirements

The support for subscriber certificates is a capability rather than a service and it can be used as a tool when mechanisms are specified to meet security requirements associated to various 3GPP work items. The capability is needed to fulfill the security objective (f) defined in TS 33.120 "3G Security principles and objectives":

" f) to ensure that the implementation of 3GPP security features and mechanisms can be extended and enhanced as required by new threats and services. "

The target is to make it possible to issue subscriber certificates in 3GPP systems in order to authorize and account for service usage both in home and in visited network. [WID]

The following requirements have been identified:

- The certificate request procedure needs to support obtaining subscriber and operator certificates from the visited network (i.e. there should be a CA in the visited network).
    - This is needed as a service provider will typically have relationship only to the local operators in his geographic region. Without a global PKI he cannot recognize certificates of a visiting user issued by the home network.
- The certificate request procedure needs to support obtaining subscriber and operator certificates from the home network (i.e. there should be a CA in the home network).
    - Some services (e.g. LCS or home network based services) may require certificates from home network.

3. Proposed actions

The identified requirements are sent to S2 and cc:ed to S1.

References

[WID] S3-020162, Support for subscriber certificates