3GPP TSG SA WG3 Security — S3#25 **S3-020463**

8 - 11 October 2002

Munich, Germany

3GPP TSG-SA-1 Meeting #17 ***S1-021685***
Durango, USA, 12-16 August 2002

Title:	**Liaison Statement on subscriber certificates**
Source:	SA1
To:	SA3, SA2, T2
Cc:	SA5

Contact Person:

Name:	Tommi Kokkola
Tel. Number:	+358 40 5040734
E-mail Address:	tommi.kokkola@nokia.com

Attachments: None

1. Overall Description:

SA1 thanks SA3, SA2 and T2 for their liaison statements about subscriber certificates.

SA1 wishes to inform that a new section has been added to TS 22.105, which is copied below:

Certificates

Certificates may be used for a global scale authorization infrastructure for various applications and services based on the 3GPP system security architecture. Services may be provided by parties that are not necessarily trusted by the cellular operators nor by cellular subscribers. Therefore technical means to securely deliver and authenticate services from other parties are necessary. 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.

In addition to these certificates, there are other types of certificates. For example, service provider certificates (provided by service providers), and third party certificates (provided by third parties, e.g. Value Added Service Providers) etc. These certificates are described and standardized by other fora such as IETF PKIX working group and WAP forum.

Authorization of such services may be based on credentials like digital signatures. The service provider and the network operator shall use subscriber certificates to verify these credentials. The UE may also use operator CA certificates and other certificates to verify the credentials supplied by service providers and third parties. 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).

Example usage scenarios of the subscriber certificate feature are payment via subscriber phone bill and location information offered by the operator to other service providers. It should be noted that the service using this feature may be outside of scope of 3GPP or implemented using existing 3GPP toolkits.
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.

For further information on certificates see TS 33.102[12].

SA1 believes that these requirements answer to questions raised by other LSs.

2. Actions:

None

3. Date of Next SA1 Meetings:

Title	Date	Location	Country
SWGs	14-18 October 2002		China