3GPP TSG SA WG3 Security — S3#23 S3-020299

14 - 17 May 2002

Victoria, Canada

Title:	Draft LS on subscriber certificates
Source:	SA3
To:	SA2, CN1
Cc:	SA1

Contact Person:

Name:	**Valtteri Niemi**
Tel. Number:	+ 358 50 48 37327
E-mail Address:	valtteri.niemi@nokia.com

Attachments: S3-020077, S3-020300

1. Overall Description:

SA3 are working on a Release 6 work item called “Support for subscriber certificates”. The objective of the work is to create a security capability for 3GPP systems that can be used to provide secure mechanisms for various applications and services.

Some example usage scenarios for these certificates are described in the attached document S3-020077.

The core of the planned new functionality is described in the attached proposed CR to TS 33.102 (3G security architecture).

It is essential for the feature that integrity protected signalling channels can be used for certificate request-response procedures. This implies that the new procedures are included as part of the UE-CN signalling, and the two procedures are specified in TS 24.008.

It is not the intention of SA3 to specify a full public key infrastructure. Instead, existing components of e.g. Wireless PKI are re-used. This limits the amount and scope of the specification work needed in 3GPP. However, a so-called Certificate Authority (CA) is needed when certificates are issued. In the proposed mechanism, the cellular core network and the PKI are associated to each other via a link between SGSN and CA.

2. Actions:

ACTION TO CN1: To study the impacts of the proposed mechanism to 24.008 and provide feed-back to SA3 as necessary;

ACTION TO SA2: To study the impacts of the proposed mechanism to the 3GPP system architecture and provide feedback to SA3 as necessary.

3. Date of Next TSG-SA3 Meetings:

SA3-24	9th – 12th July 2002	Helsinki, Finland
SA3-25	8th – 11th Oct 2002	Munich, Germany