3GPP TSG SA WG3 Security — S3#25 **S3-020479**
8 - 11 October 2002
Munich, Germany

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022051***
Miami Beach, Florida, USA, 23 – 27 September 2002

Title:	**LS response on subscriber certificates**
Response to:	LS S3-020322 on subscriber certificates from SA WG3
Release:	Rel-6
Work Item:	
Source:	CN WG1
To:	SA WG3
Cc:	

Contact Person:
Name: **Martti Perälä**
Tel. Number: +358 40 559 7034
E-mail Address: martti.perala@nokia.com

Attachments: N1-021545

---

1. Overall Description:

CN1 would like to thank SA3 for their liaison statement on subscriber certificates.

There was no study available about subscriber certificates impact to the TS 24.008 and CN1 would like to have more time to further investigate this issue.

It was noticed also that CR S3-020300 was not agreed yet in SA3, therefore CN1 would like to get more stable requirements before committing to any design.

2. Actions:

To SA3:

ACTION: To provide more stable requirements for subscriber certificates.

3. Date of Next TSG-CN1 Meetings:

CN1_Rel-6_adhoc	22nd - 24th October 2002	Munich, Germany
CN1_27	11th – 15th November 2002	Bangkok, Thailand
CN1_28	10th – 14th February 2003	Dublin, Ireland

3GPP TSG-CN1 Meeting #25 ***Tdoc N1-0211545***
Helsinki, Finland, 29 July – 2 August

Agenda item: 3 for incoming liaisons
Document for: DISCUSSION

3GPP TSG SA WG3 Security — S3#23 **S3-020322**

14 - 17 May 2002

Victoria, Canada

Title: 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) NOTE: This CR has not yet been approved by SA3.

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;

ACTIONS TO SA2:

1. To study the impacts of the proposed mechanism to the 3GPP system architecture and provide feedback to SA3 as necessary.
2. To study the need of standardisation of the interface between SGSN and CA.

3. Date of Next TSG-SA3 Meetings:

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