3GPP TSG SA WG3 Security — S3#24 **S3-020413**
9 - 12 July 2002
Helsinki, Finland

Title:	LS on architecture and requirements for subscriber certificates
Response to:	LS (S2-022047/S3-020356) on "LS on subscriber certificates" from SA2 and LS (T2-020574/S3-020333) on the same subject from T2
Release:	Release 6
Work Item:	Support for subscriber certificates
Source:	SA3
To:	SA1, SA2
Cc:	T2

Contact Person:
Name: **Valtteri Niemi**
Tel. Number: +358504837327
E-mail Address: Valtteri.niemi@nokia.com

Attachments: none

---

1. Overall Description:

SA3 thanks both SA2 and T2 for their reply LSs and their effort on identifying potential use cases for subscriber certificates.
SA3 is currently working on the following open issues under this work item:

1. Further elaboration of different usage cases and, in particular, the need of so-called "proof of possession" property in each case;
2. Compatibility with PKI solutions developed in other relevant standard fora, e.g. Mcom of ETSI, WAP Forum and IETF;
3. Comparison with conventional "global PKI" approach;
4. Implications on Lawful interception;
5. Review of different architectural solutions to support issuing of certificates;
6. Trust issues; in particular, issues related to business relationships and resolution of disputes.

SA3 will inform SA1, SA2 and T2 about conclusions on these issues.
The following answers are provided for the specific questions asked by SA2:

1. Justification of the proposal to request the subscriber certificate via the link specific access (e.g. SGSN) instead of choosing access independent method (e.g. based on IP) for requesting subscriber certificates.

Answer: Related to the issue 5 above, SA3 has discussed four alternatives on how to connect cellular network to the Certification Authority (CA):

- from SGSN
- from GGSN
- from IMS
- from a new "gateway" type element.

The proposal to choose the first alternative was presented earlier because then the procedure of issuing certificates can be integrity protected in a straightforward manner. However, SA3 acknowledges that similar level of protection may be achieved also in the other cases. Furthermore, other aspects such as the possibility to issue certificates by an access independent method have to be taken into account when final decision is made. SA3 kindly asks help from SA2 in this matter also in the future.

2. How roaming subscribers could be supported?

A: This question relates to study item 6 in the list above. Clearly, the technical solution depends on the selection between different architecture options. Also, SA3 is looking for advice from SA1 on the issue highlighted by SA2 in their LS to SA1 and SA3.

3. Security requirements related to the issuing and usage of subscriber certificates.

A: The certificate request/response messages must be authenticated and integrity-protected. The protection mechanisms for these request/response messages shall utilize the 3GPP security architecture. Further requirements may be defined as the result of the work on the areas listed above.

2. ACTIONS:

ACTIONS to SA2

SA3 kindly asks SA2 for further support on the selection between different architectural options for support of issuing certificates.

ACTIONS to SA1

SA3 kindly asks SA1 for further support on the issues highlighted by SA2. In particular, guidance is asked on what kind of control measures are needed on the home network side in the case certificates are issued for roaming subscribers.

3. Date of Next TSG-SA3 Meetings:

TSG-SA3 Meeting #25	8th – 11th October 2002	Munich, Germany.
TSG-SA3 Meeting #26	19th – 22nd November 2002	TBD