3GPP TSG SA WG3 Security — S3#22 **S3-020120**

25 - 28 February 2002

Bristol, UK

TSG-SA WG 1 (Services) meeting #15 **S1-020645**
Saalfelden, Austria, 11-15th February 2002 **Agenda Item:**

Title:	Liaison statement on support for subscriber certificates
Source:	SA1
To:	SA3
Cc:	
Response to:	

Contact Person:

Name:	Mark Cataldo
Tel. Number:	+44 777 55 8 22 88
E-mail Address:	mark.cataldo@openwave.com

Attachments:

1. Introduction

SA1 has considered the WID on *Support for subscriber certificates (S3-010704, TSGS#14(01)0622)*, and makes the following initial response.

SA1 are not aware of the requirements for this activity, and requests that SA3 identify where these may be found.

2. Mandating use of subscriber certificates

SA1 notes that the general authentication mechanism covered by this WID could be used (for example) in the following ways:-

- identify a user towards a service (3GPP standardised or VASP provided)
- enable a user to remain anonymous towards the service, whilst the user invoking the service can be identified by the network
- not require authentication at lower levels (i.e. bearer-level or signalling- levels of CS, PS and IMS)
- possibly require only insecure transport mechanisms (Internet)

SA1 currently makes no formal requirements in its technical specifications (i.e. TS 22.xxx) for the explicit support of subscriber certificates. It is considered by SA1 that potential use of subscriber certificates is a Stage 2/Stage 3 matter, and that SA1 only generates requirements which other working groups in turn could potentially support through the use of subscriber certificates.

3. Potential use of subscriber certificates

SA1 notes that there are however some technical specifications which result in certificates being required in the stage 2 and/or stage 3 specifications (an example of this, as SA3 is aware, is the MExE specification in TS23.057).

Finally, the following work items being developed by SA1 are identified which could potentially use subscriber certificates (but do not necessarily exclude consideration of others):-

- Multimedia Message Service (MMS)
    - The MMS Stage 1 requirements do not require subscriber certificates. Although not currently addressed by the MMS Stage 2, MMS could potentially consider support of PKI-based mechanisms for securing multimedia messages in the future.

- Digital Rights Management (DRM)
    - Although implementation issues are out of the scope of Stage 1, the SA1 DRM SWG believes that PKI-based mechanisms are likely to be considered in the Stage2/Stage 3 work.
- Open Service Architecture (OSA)
    - The OSA Stage 1 requirements do not require subscriber certificates. OSA could potentially be a candidate to make use of subscriber certificates in the future for support of MMS, IMS and other services.
- Generic User Profile (GUP)
    - The GUP Stage 1 requirements are still at an early stage, however it is considered that security certificates could potentially be used to support access control

4. Actions:

To SA3.

ACTION: SA1 asks SA3 to identify where the requirements for *Support for subscriber certificates* are defined. SA3 should consider how the above usage could be co-ordinated in such a way that it will allow cost efficient implementation of the security support of the UE, a 3GPP UE "security toolbox".

5. Date of Next SA1 Meetings:

Title	Date	Location	Country
SA1 Adhocs	8 – 12 Apr 02	Sophia Antipolis	France
SA1#16	13 – 17 May 02	Victoria	Canada
SA1 Adhocs	8 – 12 Jul 02		Italy
SA1#17	12 – 16 Aug 02	Durango, CO	North America
SA1 Adhocs	14 - 18 Oct 02		
SA1#18	11-15 Nov 02		