

**3GPP TSG SA WG3 Security — S3#29**  
**15 - 18 July 2003**  
**San Francisco, USA**

**S3-030439**

---

**Title:** Reply to Letter "3GPP Dependencies on OMA Deliverables" (S3-030339)  
**Release:** Rel-6  
**Work Item:** Support for Subscriber Certificates

**Source:** SA WG3  
**To:** Mr. Iain Sharp ([isharp@nortelnetworks.com](mailto:isharp@nortelnetworks.com)),  
**Cc:** -  
**Attachment:** -

**Contact Person:**

**Name:** Tao Haukka  
**Mobile Number:** +358 40 5170079  
**E-mail address:** [tao.haukka@nokia.com](mailto:tao.haukka@nokia.com)

---

Dear Mr. Iain Sharp,

SA3 would like to thank for the letter and effort on co-ordination to OMA.

Based on discussion in SA3 #29 meeting, SA3 have agreed their position on 3GPP feature "Support for Subscriber Certificates" as such, that SA3 will re-use OMA specifications that are already completed at the moment, so there is no dependency to OMA specifications development. On the other hand, there are two aspects to be addressed:

- a) SA3 establishes security element bootstrapping from AKA mechanism that is shared between smart card inserted to user equipment and the operator's network. OMA may have interests to use this mechanism to enable subscriber authentication based on AKA;
- b) SA3 TS specifies how to acquire a certificate for a public key. The key pair could be either pre-installed or locally generated. The former case is fully specified in existing OMA WIM specification. The later case is on-going in OMA SEC group under work item "On Board Key Generation and Key Enrollment", so SA3 have interests to adopt the solution and specification for on-board key generation when they are mature in the future.

SA3 have currently a plan to organize a joint meeting with OMA SEC group earliest in November, 2003. This shall be discussed in SA #21 plenary meeting in September.

SA3 point out that OSA work item in 3GPP may have dependency to OMA. However it is out of responsibility of SA3.

Please also find the table entry related to this 3GPP feature, as well as SA3 future meetings for your information.

Best regards,  
SA3

Further information:

<b>3GPP Feature</b>	<b>OMA Dependency</b>	<b>3GPP Impact if not done</b>	<b>3GP P WG</b>	<b>OMA WG</b>	<b>3GPP Plan. Release</b>	<b>OMA Plan. Date</b>	<b>Comments</b>
Subscriber Certificates	None	SA3 relies on OMA specifications	SA3	OMA SEC/SC T WG	Release 6	no information	

SA3 future meetings:

Meeting	Time	Venue
SA3 Ad Hoc	3-4 Sep. 2003 (TBC)	Europe (TBC)
SA3#30	6-10 Oct. 2003	Portugal
SA3#31	18-21 Nov. 2003	London