3GPP TSG SA WG3 Security — S3#29   **S3-030435**
15 - 18 July 2003
San Francisco, USA

LIAISON STATEMENT

Title:	Mobile PKI service enabler
To:	3GPP TSG SA WG3 and 3GPP2 TSG-S WG4
Source:	OMA SEC/SCT WG
Contact(s):	Herve BRUGAL Gemplus
	+ 33 (0) 4 42 36 60 24
	herve.brugal@gemplus.com
Attachments:	n/a

1   Overview

OMA SEC group has released a complete set of specifications to enable mobile PKI based services and applications.

This set of enabler specifications covers:

1. Mobile device security element
2. Security element bootstrapping
3. User enrolment mechanisms
4. Certificate profile
5. CRL profile and OCSP mobile profile
6. End-to-end transport layer security
7. Application layer digital signature

Based on the 3GPP SA3's work item SP-010622_S3-010704 on "Support for subscriber certificate," OMA SEC understands that the main work item's goal is to address topics (2), (3) & (4) above, while leveraging existing 3G-network infrastructure and authentication protocols.

2   Proposal

OMA proposes that all three organizations (3GPP, 3GPP2 and OMA) collaborate to progress this work item. As an initial step, OMA SEC proposes that progress reports and development plans are shared in order to identify areas of potential overlap and/or reuse.

3   Requested Action(s)

OMA SEC would be pleased to provide and discuss the set of specifications that they have issued to address the above topics.

OMA SEC would be interested to evaluate how the work they have done on items (2), (3) & (4) could fit with the work currently being done by 3GPP SA3 and 3GPP2 TSG-S WG4.

OMA SEC would also appreciate if 3GPP SA3 can elaborate on their current plans to address topics (1), (5), (6) and (7).

4   Conclusion

OMA SEC proposes close collaboration among 3GPP, 3GPP2 and OMA with the expectation that this collaboration will promote finding the best solution to support subscriber certificates.