3GPP TSG-SA WG3 Meeting S3#33
Beijing, China, May 10-14, 2004

Tdoc ⌘S3-040292

CR-Form-v7

CHANGE REQUEST

⌘ **33.221** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Editorial change to correct the reference's sources
Source:	⌘	Nokia
Work item code:	⌘	SSC
Date:	⌘	24/04/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Several OMA, original WAP references have been moved to from their earlier location due to reorganization of OMA, therefore the references are updated; Reference 2 and 3 are removed since the corresponding technology was decided not to include in the present specification.
Summary of change:	⌘	Removal of obselete references; correction of reference format and refer to public available material of OMA.
Consequences if not approved:	⌘	Unclear sources to the audience.

Clauses affected:	⌘	2, 4.5.1.2.2

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] PKCS#10 v1.7: "Certification Request Syntax Standard", RSA Laboratories, May 2000.

[2] ~~Adams C., Farrell S.: "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.~~void

[3] ~~Myers M., et al.: "Internet X.509 Certificate Request Message Format", RFC 2511, March 1999.~~void

[4] Chokhani S., et al.: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 2527, March 1999. IETF.

[5] Franks J., et al.: "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999. IETF.

[6] Housley R., et al.: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002. IETF.

[7] WAP-211-WAPCert, 22.5.2001: http://www.openmobilealliance.org/tech/affiliates/wap/WAP-211-WAPCert-20010522-a.pdf~~http://www1.wapforum.org/tech/terms.asp?doc=WAP-211-WAPCert-20010522-a.pdf~~, Open Mobile Alliance.

[8] WAP-260-WIM-20010712, 12.7.2001: http://www.openmobilealliance.org/tech/affiliates/wap/WAP-260-WIM-20010712-a.pdf~~http://www1.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf~~, Open Mobile Alliance.

[9] WAP-217-WPKI, 24.4.2001: http://www.openmobilealliance.org/tech/affiliates/wap/WAP-217-WPKI-20010424-a.pdf~~http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf~~, Open Mobile Alliance.

[10] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997: "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", 1997.

[11] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[12] 3GPP TS 33.222: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Function using HTTPS".

[13] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System description".

[14] OMA:~~Open Mobile Alliance~~ ECMA Crypto Library, OMA-WAP-ECMACR-V1_1-20040326-C.zip, http://member.openmobilealliance.org/ftp/Public_documents/SEC/Permanent_documents/, Open Mobile Alliance. ~~http://www.openmobilealliance.org~~.

[15] Blake-Wilson, S., et al, "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003. IETF.

[16] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[17] Santesson, S., Polk, W., Barzin, P., and M. Nystrom, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", RFC 3039, January 2001. IETF.

[18] ETSI TS 101 862: "Qualified certificate profile".

[19] OMA: "Provisioning Content Version 1.1", Version 13-Aug-2003. Open Mobile Alliance.

*** NEXT CHANGE ***

4.5.1.2.2 Key Generation

If the private key is stored in a UICC (e.g. in a WIM) and the UICC demands a special authorization (e.g. from the Operator) to generate the key, the ME may need to perform an HTTP POST request, which MAY be authenticated and integrity protected by HTTP Digest Authentication, to the NAF in order to deliver a nonce that is generated by the UICC. This will allow the NAF to authenticate directly to the UICC application and provide authorization for the key generation. The exact key generation procedure is specified in ECMA Crypto Library [14].

~~Editor's note: A reference to the relevant OMA specifications should be added.~~

*** END OF CHANGE ***