3GPP TSG SA WG3 Security — S3#36
Shenzhen, China, 23–26 November 2004

Tdoc ⌘S3-041100

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **019** ⌘ **rev** **2** ⌘ Current version: **6.2.1** ⌘

*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 [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Profile for PDG certificates in Scenario 3
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	07/09/2004
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	33.234 says PDG is authenticated with certificates, but does not specify how the certificates are handled.
Summary of change:	⌘	Specifies the contents of PDG certificates and requirements for their processing at the WLAN UE.
Consequences if not approved:	⌘	Reduced interoperability.

Clauses affected:	⌘	2, 6.1.5, new clause between 6.6 and 6.7

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

Other comments: ⌘

********** FIRST CHANGE **********

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] 3GPP TR 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] IETF RTC 3748: "Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".

[8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[14] RFC 2486, January 1999: "The Network Access Identifier".

[15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

[16] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[17] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.

[18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.

[23] draft-ietf-aaa-eap-08.txt, June 2004: "Diameter Extensible Authentication Protocol (EAP) Application". IETF Work in progress

[24] RFC 3588, September 2003: "Diameter base protocol".

[25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[27] draft-ietf-eap-keying-02.txt, June 2004: "EAP Key Management Framework". IETF Work in progress

[28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-06.txt, April 2004: "Cryptographic Suites for IPsec". IETF Work in progress

[32] draft-ietf-ipsec-udp-encaps-09.txt, May 2004: "UDP Encapsulation of IPsec Packets". IETF Work in progress

[33] draft-ietf-ipsec-ikev2-algorithms-05.txt, April 2004: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2". IETF Work in progress

[34] RFC 2104, February 1997: "HMAC: Keyed-Hashing for Message Authentication".

[35] RFC 2404, November 1998: "The Use of HMAC-SHA-1-96 within ESP and AH".

[36] RFC 2548, March 1999: " Microsoft Vendor-specific RADIUS Attributes".

[37] draft-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

[38] RFC 3279, April 2002: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[39] RFC 3280, April 2002: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

********** NEXT CHANGE **********

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- The WLAN-UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG. The PDG shall authenticate itself with an identity, for example, "pdg.mncNNN.mccMMM.3gppnetwork.org". This identity shall be contained in the IKEv2 ID_FQDN payload and shall match a dNSName SubjectAltName component in the PDG's certificate. A profile for certificate contents and processing is defined in section 6.x.
- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN-UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN-UEs, which contain a SIM and no USIM.
- A profile for IKEv2 is defined in section 6.5.

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.

********** FINAL CHANGE **********

Insert new section below after 6.6 (Profile for IPsec ESP) but before 6.7 (WLAN UE split interworking)

6.x Profile for PDG certificates

Certificates used for authentication of the PDG shall meet the following profile of RFC 3280 [39].

a) The certificate shall be encoded in DER format.

b) The version shall be 2 ("v3").

c) The certificate serial number shall meet the requirements in RFC3280 [39], section 4.1.2.2.

d) The signature algorithm shall be "sha1WithRSAEncryption" [38], and the RSA public key used for signing shall not be longer than 2048 bits.

e) The issuer name shall not be empty.

f) The validity period shall meet the requirements in RFC3280 [39], section 4.1.2.5.

f) The subject name may be empty in PDG certificates and shall not be empty in CA certificates.

g) The subject public key shall use algorithm "rsaEncryption" (RFC3279 [38]), and the RSA public key shall not be longer than 2048 bits.

h) The issuerUniqueID or subjectUniqueID fields shall not be present.

i) The SubjectAltName extension shall be present if this is a PDG certificate, and shall contain at least one dNSName component.

j) The BasicConstraints extension shall be present if this is a CA certificates with "CA" flag asserted. The pathLenConstraint may be present.

k) CA certificates should contain the NameConstraints extension with appropriate dNSName components in the permittedSubtrees field.

l) The KeyUsage extension shall be present in all certificates. The keyCertSign bit shall be set in CA certificates, and digitalSignature bit shall be set in PDG certificates.

m) The CRLDistributionPoint extension may be present, and shall not be marked critical. At least one of the distribution points should use HTTP for retrieving the CRL.

n) The AuthorityInformationAccess extension may be present with id-ad-ocsp access method, and shall not be marked critical.

o) Other extensions should not be used; if they are, they shall not be marked as critical.

p) The total length of a certificate shall not exceed 2000 bytes.

Certificate processing requirements:

a) UE shall send one or more CERTREQ payloads with encoding value 4 (X.509 certificate - Signature).

b) IKEv2 Certificate encoding value shall be 4 (X.509 certificate - Signature).

c) UE shall not assume that any except the first IKEv2 CERT payload is ordered in any way.

d) UE shall support paths of at least four certificates (self-signed CA certificate, intermediate CA 1, intermediate CA 2, PDG certificate).

e) PDG shall not send paths containing more than four certificates.

f) UE shall be prepared to receive irrelevant certificates, or certificates they do not understand.

g) UE shall be able to process certificates (for e.g. chain building) even if naming attributes are unknown.

h) UE shall support both UTCTime and GeneralizedTime encoding for validity time.

i) UE shall check the validity time, and reject certificates that are either not yet valid or are expired.

j) UE shall support processing of the BasicConstraints, NameConstraints, and KeyUsage extensions.

k) UE may check the validity of the certificates using CRLs or OCSP. Support for CRLs is optional. Support for OCSP is mandatory.

********** END OF CHANGE **********