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

Tdoc S3-041110

CR-Form-v7.1

CHANGE REQUEST

33.234	CR	042	rev	1	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:	Fallback from re-authentication to full authentication
Source:	SA WG3
Work item code:	WLAN
Date:	25/11/2004
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:	Currently in TS 33.234 it is described how to force a re-authentication process from a full authentication (sending a re-authentication identity from the AAA server), but it is not clearly described how to request again a full authentication when re-authentications have been started
Summary of change:	It is indicated in the TS that, in order to be able to perform a full authentication after a re-authentication, the AAA server has to issue a pseudonym together with a re-authentication id. The AAA server, when it decides to have full authentication, will reject the re-authentication identity and request the pseudonym
Consequences if not approved:	Fallback from fast re-authentication to full authentication may be performed using the permanent user identity (IMSI), which is not desirable from identity privacy perspective. The fallback process is not currently described properly in the TS and implementations may vary.

Clauses affected:	2, 6.1.4.2 (new)

Other specs affected:	Y	N		
	X		Other core specifications	24.234
		X	Test specifications	
		X	O&M Specifications	

Other comments:	

*** BEGIN SET OF CHANGES ***

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~~13, ~~April~~ October 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-~~13~~14, ~~April~~ October 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".

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.4.2 Fallback to full authentication from fast re-authentication

In the EAP SIM/AKA processes for full authentication, the 3GPP AAA server sends to the WLAN UE the temporary identities to be used in the next authentication process. This next authentication process may be either a full authentication process or a fast re-authentication process, depending on the type of temporary identity received by the WLAN UE. If the WLAN UE receives a fast re-authentication identity, it shall use it in the next authentication, thus indicating to the AAA server that a fast re-authentication must be performed. If the WLAN UE receives only a pseudonym, the WLAN UE shall use it in the next authentication process and hence a full authentication will be started.

Whenever a fast re-authentication identity is received by the WLAN UE, this shall be the temporary identity used in the next authentication process, regardless if a pseudonym was received as well. The full authentication EAP Request/SIM Challenge and EAP Request/AKA Challenge messages allow both types of identity to be sent. However, in the messages EAP Request/AKA Re-authentication and EAP Request/SIM Re-authentication it is possible to send only re-authentication identities, according to ref. [4] and [5].

If the home network decides to initiate fast re-authentications, it shall indicate it to the WLAN UE by means of including the fast re-authentication identity in a full authentication process. If, later on, the home network decides to perform again full authentication, the 3GPP AAA server shall indicate it to the WLAN UE requesting a pseudonym after reception of the re-authentication identity. For this reason, whenever the AAA server sends a fast re-authentication identity to the WLAN UE, it shall include as well a pseudonym, so that the WLAN UE keeps it in case of fallback to full authentication, requested by the AAA server.

In case of EAP AKA, the AAA server, when it decides to perform full authentication again, shall use the message EAP Request/AKA Identity with the parameter AT_FULLAUTH_ID_REQ. The WLAN UE shall then return the pseudonym according to ref. [4].

In case of EAP SIM, the AAA server, when it decides to perform full authentication again, shall use the message EAP Request/SIM/Start with the parameter AT_FULLAUTH_ID_REQ. The WLAN UE shall then return the pseudonym, according to ref, [5].

*** END SET OF CHANGES ***