**3GPP TSG SA WG3 Security — S3#34** *Tdoc ⌘S3-040511*
**Acapulco, Mexico 6 – 9 July 2004**

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Example of using EAP-AKA/EAP-SIM within IKEv2 for Mutual Authentication between UE and PDG |
| ***Source:*** | ⌘ | Samsung, Huawei |
| ***Work item code:*** | ⌘ | WLAN |
| ***Date:*** | ⌘ | 23/06/2004 |
| ***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:*** | ⌘ | In IKEv2 internet drafts, it is stated that EAP methods within IKEv2 can be used for mutual authentication of the peers before forming the IPSec security association. But there is no standard available on how this authentication procedure will be performed between WLAN UE, PDG and AAA server and how these EAP packets are carried between PDG and the AAA Server. |
| ***Summary of change:*** | ⌘ | This Annexure discusses the procedure to use IKEv2 in association with EAP between a WLAN UE and PDG, to perform mutual authentication of UE and PDG. |
| ***Consequences if not approved:*** | ⌘ | There should be a standandard procedure to define EAP within IKEv2 procedure between a WLAN UE, PDG and AAA Server and how mutual authentication is performed between UE and PDG for IKEv2. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | |
| ***Other specs affected:*** | ⌘ | Y N<br>[ ] [X] Other core specifications<br>[ ] [X] Test specifications<br>[ ] [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] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-12, October 2003: "EAP SIM Authentication".

[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-03.txt, October 2003: "Diameter Extensible Authentication Protocol (EAP) Application".

[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-01.txt, November 2003: "EAP Key Management Framework".

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

[29] draft-ietf-ipsec-ikev2-1~~3~~4.txt, Ma~~rch~~y 2004: "Internet Key Exchange (IKEv2) Protocol".

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

[31] draft-ietf-ipsec-ui-suites-05.txt, April 2004: "Cryptographic Suites for IPsec".

[32] draft-ietf-ipsec-udp-encaps-09~~8~~.txt, ~~February~~ May 2004: "UDP Encapsulation of IPsec Packets".

[33] draft-ietf-ipsec-ikev2-algorithms-04.txt, September 2003: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2".

[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".

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

# Annex G: (informative): Example of using EAP-AKA/EAP-SIM within IKEv2 for Mutual Authentication to create a IPSec Security Association for a Tunnel between UE and PDG.

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.

The IETF draft for IKEv2 [ref 29] uses AUTH for mutual authentication of the peers before forming the IPSec security association. This AUTH parameter is calculated based on a shared secret between the two peer entities. This shared secret can be either a pre-shared key, public key signatures or can be obtained through EAP procedures. This Annexure discusses the procedure to use IKEv2 in association with EAP between a WLAN UE and PDG, to perform mutual authentication of peers ( UE and PDG).
In IKEv2 a special payload type "EAP payload " is defined for allowing EAP messages within IKEv2. Between the PDG and the AAA Server, EAP messages are typically encapsulated in an AAA protocol, e.g. in DIAMETER (see figure G.1).


**Figure G.1: Example of mutual authentication for IKEv2 using EAP-AKA/EAP-SIM**

Examples of EAP methods (RFCs or Internet Drafts) are:

- EAP-SIM for SIM-based authentication. (Internet Draft) (Ref. [5]);
- EAP-AKA for SIM and USIM-based authentication (Internet Draft) (ref. [4]);

The actual EAP authentication takes place between the UE and the AAA Server and is in principle transparent to the PDG. The PDG only has to forward all EAP messages between the UE and the corresponding AAA server. The EAP payloads within the IKEv2 message from the UE shall be extracted and sent over DIAMETER to the AAA server. Similarly the EAP messages from the AAA server shall be extracted from the DIAMETER and shall be sent to the UE encapsulated within IKEv2 messages. At the end of the EAP procedure, if authentication is successful, the AAA server sends a DIAMETER Access Accept message to the PDG (in the case DIAMETER is used as AAA protocol) with the session keys and EAP-Success as the attributes in the DIAMETER Access Accept message. The PDG then knows that the UE has been authenticated and uses the MSK received in the session keying material of the DIAMETER Access Accept message as the shared secret to calculate the AUTH value for mutual authentication. The PDG also sends the received EAP-Success message to the UE within IKEv2. The UE will also use the derived MSK as the shared secret to calculate AUTH value required for IKEv2 mutual authentication.

*** END SET OF CHANGES ***