3GPP TSG SA WG3 Security#31 **S3-030748**
18-21 November, 2003
Munich, Germany

Agenda Item: **6.10 (WLAN)**

Source: **Siemens**

Title: **Security procedures for the set up of UE-initiated tunnels in scenario 3**

Document for: **Discussion and decision**

Abstract

At SA3#30, Siemens presented the contribution S3-030550 on "Evaluation of alternatives for secure set-up of UE initiated tunnels". It is proposed in this contribution to select the alternative preferred in S3-030550, namely IKEv2 with EAP-based UE authentication, as a working assumption of SA3 and include corresponding text in the main body of draft TS 33.234. It is also proposed to further study alternatives and include corresponding text in an annex of draft TS 33.234. An accompanying pseudo-CR to TS 33.234 v070 implements these proposals. The pseudo-CR also implements the working assumptions on the use of IPsec ESP agreed at SA3#30 and proposes some changes to the structure of the TS.

1. Conclusions of S3-030550

S3-030550 on "Evaluation of alternatives for secure set-up of UE initiated tunnels" reached the following conclusions:

- "... it appears that, from a technical point of view, IKEv2 with EAP-based authentication of the UE is the preferable solution.
- It remains to be decided by SA3, however, whether IKE should be preferred because of existing product implementations.
- If IKE was preferred for this reason then this seems to contradict 3GPP-specific additions to IKE implementations for key management as this would also mean the development of new products. However, the effort to get such additions in place is certainly a factor to be considered further.
- A decision for IKE as available today would mean the introduction of subscriber certificates. SA3 (especially operators) need to decide whether the deployment of subscriber certificates for the purposes of scenario 3 is considered feasible and desirable.
- As usual, several options in the standard should be avoided."

S3-030550 dealt mainly with the key management-related properties of IKE and IKEv2. S3-030557, also presented at SA3#30, argued in favour of IKEv2 due to other properties of IKEv2. This should also be taken into account. Other contributions have not been presented to SA3 on this issue so far.

2. Proposal for a working assumption on tunnel set-up

As draft TS 33.234 needs to be presented to SA for information in December 2003, draft TS 33.234 needs to contain at least the outline architecture for the scenario 3 part, i.e. for the security procedures to set up UE-initiated tunnels. Therefore, it is considered necessary that SA3 agrees on a working assumption with the understanding that other alternatives may be studied further and that these alternatives may replace the working assumption if SA3 finds problems with the working assumption.

- The proposed working assumption is IKEv2 with EAP-based authentication of the UE and certificate-based authentication of the PDG.
- Alternatives for further study are IKE and IKEv2 with subscriber certificates.

Other alternatives may also be studied further if SA3 agrees to do so.

3. Proposed CR to TS 33.234 v070

It is proposed that SA endorses the accompanying CR. This CR implements three types of changes:

- Changes to headlines of existing sections and introduction of new subsections to make room for the specification of the security for scenario 3 in TS 33.234. These affect sections 4, 5, and 6.1.1 through 6.1.4 of TS 33.234.
- Changes agreed at SA3#30 regarding the use of IPsec ESP for data protection in the tunnel. These affect sections 6.2, 6.3, and 6.6 (new) of TS 33.234.
- The working assumption on tunnel set up procedures proposed in section 2 of this contribution. These affect sections 6.1.5 (new), 6.5 (new) and Annex X (new) of TS 33.234.

3GPP TSG SA WG3 Security — S3#31 **att_S3-030748**
18 – 21 November, 2003, Munich, Germany

CR-Form-v7

Pseudo - CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.7.0 ⌘

*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:	⌘	Security procedures for UE-initiated tunneling
Source:	⌘	Siemens
Work item code:	⌘	WLAN
Date:	⌘	18 Nov 2003
Category:	⌘	**C**
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:	⌘	SA3 needs to include at least an outline architecture for the security procedures for scenario 3 before the TS is presented to SA in December
Summary of change:	⌘	IKEv2 with EAP user authentication is included in the main body as working assumption, IKE and IKEv2 with subscriber certificates are included as alternatives in annexes
Consequences if not approved:	⌘	If there are no other CRs at SA#31 proposing security procedures for scenario 3: the TS may not be sufficiently complete to be forwarded to SA in December; If there are other CRs at SA#31 proposing security procedures for scenario 3 of a similar level of detail: SA3 needs to select one of them or merge them.

Clauses affected:	⌘				
		Y	**N**		
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘ TS 23.234 CN1 and CN4 specs
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

***** Begin of Change ****

4.2.6 UE-initiated tunneling

The security features that are expected in a tunnel from the UE to the VPLMN or HPLMN will be:

- Data origin authentication and integrity must be supported.
- Confidentiality must be supported.
- The 3GPP network has the ultimate decision to allow tunnel establishment, based on:
  - The level of trust in the WLAN AN and/or VPLMN
  - The capabilities supported in the WLAN UE
  - Whether the user is authorized or not to access the services (in the VPLMN or HPLMN) the tunnel will give access to.
- The 3GPP network, in the setup process, decides the characteristics (encryption algorithms, protocols,...) under which the tunnel will be established.

Note: Authorization for the tunnel establishment is decided by the 3GPP AAA and enforce by the PDGW or WAG. Whether this authorization information is protected or not is FFS.

Working assumptions:

~~1.IPsec ESP will be used to protect the tunnels between UE and PDG required by scenario 3.~~

~~2.~~1. The security mechanisms used in context with the IP tunnel in scenario 3 are to be independent of the link layer security in scenario 2. [Editors note: The independence requirement is not for security reasons). If the solution developed implies significant inefficiencies then this would be reported to SA WG2 for possible revision of this independence requirement.]

~~3.~~2. ~~Further study will concentrate on IKE and IKEv2 for setting up the keys for IPsec ESP.~~

~~Further work identified for SA3~~

~~1.Define a profile of IPsec ESP for use with scenario 3.~~

~~2.~~1. ~~Standardise the set-up of security associations for IPsec ESP between UE and PDG.~~

***** End of Change ****

***** Begin of Change ****

5.1 Authentication of the subscriber and the network and Security Association ~~Key~~ Management

[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network. The authentication and key management mechanisms fulfilling the requirements in chapter 4 shall be listed here]

5.1.1 End to End WLAN Access Authentication (Scenario 2)

WLAN access ~~A~~authentication signalling is executed between WLAN-UE and 3GPP AAA Server. This authentication signalling shall be independent on the WLAN technology utilised within WLAN Access network.. WLAN

authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284 (ref. [3])

5.1.2 Transport of WLAN access authentication signalling over the WLAN Radio interface

WLAN authentication signalling is carried between WLAN-UE and WLAN Access Network by WLAN Access Technology specific protocols. These WLAN technology specific protocols shall be able to meet the security requirements set for WLAN Access control in 3GPP-WLAN interworking. To ensure multi-vendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology. For IEEE 802.11 type of WLAN radio interfaces the WLAN radio interface shall conform to IEEE 802.11i standard (ref. [6]).

5.1.3 Transport of WLAN access authentication signalling between the WLAN access network and the 3GPP AAA proxy server

WLAN Authentication signalling shall be transported over Wr reference point by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network. The transport of Authentication signalling over Wr reference point shall be based on standard Diameter or RADIUS protocols.

5.1.4 Transport of WLAN access authentication signalling between the 3GPP AAA proxy server and the 3GPP AAA server

WLAN Authentication signalling shall be transported over Ws reference point by standard mechanisms.

5.1.5 Transport of WLAN access authentication signalling between the 3GPP AAA server and the HSS

WLAN Authentication signalling shall be transported over Wx reference point by standard mechanisms.

5.1.6 User Identity Privacy in WLAN access

User identity privacy (Anonymity) is used to avoid sending the cleartext permanent subscriber identity (NAI) and make the subscriber's connections unlinkable to eavesdroppers.

User identity privacy is based on temporary identities, or pseudonyms. The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementations, but optional for use.

The AAA server generates and delivers the pseudonym to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the pseudonym, it will just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the pseudonym.

To avoid user traceability, the user should not be identified for a long period by means of the same temporary identity. On the other hand, the AAA server should be ready to accept at least two different pseudonyms, in case the WLAN-UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain more than one allowed pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user to send its permanent identity. This represents a breach in the provision of user identity privacy. It is a matter of the operator's security policy whether to allow clients to accept requests from the network to send the cleartext permanent identity. If the client rejects a legitimate request from the AAA server, it will be denied access to the service.

[Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.]

5.1.7 Re-authentication in WLAN access

WLAN re-authentication is performed between WLAN-UE and AAA server, through Ws and Wr interfaces.

The WLAN-AN can initiate the re-authentication process periodically. The frequency of the re-authentications is determined by a counter which normally is set by O&M procedures in the WLAN-AN but it can be sent to the WLAN-AN by the AAA server in a RADIUS or Diameter message (in the attribute Session Timeout). At reception of this attribute, the WLAN-AN may substitute the previously set counter by the received one. Nevertheless, the 3GPP network does not have the certainity that the counter sent by the AAA server is enforced by the WLAN AN, since the latter may not support this feature (the reception and acceptance of the Session Timeout attribute). In this case, the WLAN AN will discard it and trigger the re-authentications in the period set by O&M procedures as mentioned before.

The re-authentication process initiated by the WLAN-AN will be performed either with a full authentication process or with a fast re-authentication process (from now on it will be simply called re-authentication). When the process is triggered by the WLAN AN, it is the client's decision to perform either a full authentication or a re-authentication (fast). This is indicated to the WLAN AN by sending either a pseudonym (full authentication) or a re-authentication id (fast). Both processes are described in this TS.

The re-authentication process must be implemented together with the full authentication procedure, although its use is optional and depends on operators' polices. These policies depend on the level of trust of the 3GPP operator and the WLAN AN, and the possible threats detected by operator which may require a periodic refresh of keys. The full process description can be found in ref. [4] and [5].

Note: it is still pending to define how the re-authentication id is generated.

5.1.8 Security Association Management for UE-initiated tunnels (Scenario 3)

- The tunnel endpoints, the UE and the PDG, are mutually authenticated when setting up the tunnel;
- The tunnel set-up procedure results in security associations which are used to provide confidentiality and integrity protection, as required according to sections 5.2 and 5.3, for data transmitted through the tunnel.

5.2 Confidentiality protection

[Editor's note: This section shall deal with what confidentiality protection that is provided between different nodes both inter domain, intra domain and the WLAN-UE. It shall justify the selected mechanisms (hop-by-hop or end-to-end) and protection at different layers]

5.2.1 Confidentiality protection in scenario 2

text to be added

5.2.2 Confidentiality protection in scenario 3

It shall be possible to protect the confidentiality of IP packets sent through a tunnel between the UE and the PDG.

5.3 Integrity protection

[Editor's note: This section shall deal with what integrity protection that is provided between different nodes both inter domain, intra domain and the WLAN-UE. It shall justify the selected mechanisms (hop-by-hop or end-to-end) and protection at different layers]

5.3.1 Integrity protection in scenario 2

text to be added

5.3.2 Integrity protection in scenario 3

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected.

***** End of Change ****

***** Begin of Change ****

6.1.1 USIM-based WLAN Access Authentication

***** End of Change ****

***** Begin of Change ****

6.1.2 GSM SIM based WLAN Access authentication

***** End of Change ****

***** Begin of Change ****

6.1.4 Re-authentication mechanisms in WLAN Access

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

- The 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.
- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate 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 X. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex X will be removed before the TS is submitted for approval.

6.2 Confidentiality mechanisms

~~[Editor's note: This section shall deal with cipher algorithms]~~

6.2.1 Confidentiality mechanisms in scenario 2

text to be added

6.2.2 Confidentiality mechanisms in scenario 3

The confidentiality of IP packets sent through a tunnel between the UE and the PDG, if required, shall be protected by IPsec ESP [rfc2406]. A profile for IPsec ESP is defined in section 6.6.

6.3 Integrity mechanisms

6.3.1 Integrity mechanisms in scenario 2

text to be added

6.3.2 Integrity mechanisms in scenario 3

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected by IPsec ESP [rfc2406]. A profile for IPsec ESP is defined in section 6.6.

~~[Editor's note: This section shall deal with integrity algorithms]~~

***** End of Change ****

***** Begin of Change ****

6.5 Profile of IKEv2

IKEv2, as specified in [ikev2], contains a number of options which are not all needed for the purposes of this specification. IKEv2ESP is therefore profiled in this section. When IKEv2 is used in the context of this specification the profile specified in this section shall be supported.

Editor's note: an example of a profile of IKE, which may be useful to study when writing this section, can be found in TS 33.210, section 5.4.

6.6 Profile of IPsec ESP

IPsec ESP, as specified in [rfc2406], contains a number of options which are not all needed for the purposes of this specification. IPsec ESP is therefore profiled in this section. When IPsec ESP is used in the context of this specification the profile specified in this section shall be supported.

Editor's note: an example of a profile of IPsec ESP, which may be useful to study when writing this section, can be found in TS 33.210, section 5.3.

***** End of Change ****

***** Begin of Change ****

Annex X: Alternative Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

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 X. 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.

Annex X1: IKE with subscriber certificates

- The UE and the PDG use IKE, as specified in [rfc2409], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in [rfc2409], is used in order to authenticate the PDG and the UE.
- A profile for IKE is defined in section 6.5.

Annex X2: IKEv2 with subscriber certificates

- The 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 in order to authenticate the PDG and the UE.
- A profile for IKEv2 is defined in section 6.5.

***** End of Change ****