CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.210** **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 ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Use of IPsec ESP with encryption on the Za-interface
Source:	⌘	Siemens
Work item code:	⌘	NDS/IP
Date:	⌘	5/5/2003
Category:	⌘	**A**
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:	⌘	There is a contradictory statement on use of IPsec ESP on the Za-interface. It currently states that on the Za-interface ESP shall be used with encryption but at the same time usage without encryption is allowed.
Summary of change:	⌘	Specify for Za-interface that ESP integrity/authentication is mandatory to use and encryption is recommended to use. The sequence of the sentences is rearranged to enhance reading.
Consequences if not approved:	⌘	The specification will stay inconsistent.

Clauses affected:	⌘	5.6.2

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

Other comments:	⌘	

*****first change *****

5.6.2 Interface description

The following interfaces are defined for protection of native IP based protocols:

- **Za-interface (SEG-SEG)**

  The Za-interface covers all NDS/IP traffic between security domains. On the Za-interface, authentication/integrity protection is mandatory and encryption is recommended. ESP shall be used for providing authentication/integrity protection and encryption. The SEGs use IKE to negotiate, establish and maintain a secure ESP tunnel between them. ~~Inter-SEG tunnels can be available at all times, but they can also be established as needed. ESP shall be used with both encryption and authentication/integrity, but an authentication/integrity only mode is allowed.~~ The tunnel is subsequently used for forwarding NDS/IP traffic between security domain A and security domain B. Inter-SEG tunnels can be available at all times, but they can also be established as needed.

  One SEG of security domain A can be dedicated to only serve a certain subset of security domains that security domain A needs to communicate with. This will limit the number of SAs and tunnels that need to be maintained.

  All security domains compliant with this specification shall operate the Za-interface.

- **Zb-interface (NE-SEG / NE-NE)**

  The Zb-interface is located between SEGs and NEs and between NEs within the same security domain. The Zb-interface is optional for implementation. If implemented, it shall implement ESP+IKE.

  On the Zb-interface, ESP shall always be used with authentication/integrity protection. The use of encryption is optional. The ESP Security Association shall be used for all control plane traffic that needs security protection.

  Whether the Security Association is established when needed or a priori is for the security domain operator to decide. The Security Association is subsequently used for exchange of NDS/IP traffic between the NEs.

NOTE 1: The security policy established over the Za-interface may be subject to roaming agreements. This differs from the security policy enforced over the Zb-interface, which is unilaterally decided by the security domain operator.

NOTE 2: There is normally no NE-NE interface for NEs belonging to separate security domains. This is because it is important to have a clear separation between the security domains. This is particularly relevant when different security policies are employed whithin the security domain and towards external destinations.

The restriction not to allow secure inter-domain NE-NE communication does not preclude a single physical entity to contain both NE and SEG functionality. It is observed that SEGs are responsible for enforcing security policies towards external destinations and that a combined NE/SEG would have the same responsibility towards external destinations. The exact SEG functionality required to allow for secure inter-domain NE←→NE communication will be subject to the actual security policies being employed. Thus, it will be possible to have secure direct inter-domain NE←→NE communication within the framework of NDS/IP if both NEs have implemented SEG functionality. If a NE and SEG is combined in one physical entity, the SEG functionality of the combined unit should not be used by other NEs towards external security domains.