Technical Specification Group Services and System Aspects **TSGS#19(03)0104**

Meeting #19, Birmingham, UK, 17-20 March 2003

Source: **SA WG3**

Title: **2 CRs to 33.210: Za-interface and roaming agreements (Rel-5, Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were approved by SA WG3 meeting #27 and are hereby presented to TSG SA#19 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030104	33.210	005	-	Rel-5	Add protected port into Via header	F	5.2.0	SEC-NDS-IP	S3-030127
SP-030104	33.210	006	-	Rel-6	Add protected port into Via header	A	6.0.0	SEC-NDS-IP	S3-030128

3GPP TSG-SA3#27 **Tdoc ⌘S3-030127**
Sophia Antipolis, France, 25-28 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **005** ⌘**rev** **-** ⌘ Current version: **5.2.0** ⌘

*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:	⌘	Za-interface and roaming agreements
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	26/2/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

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 case two SEG's interconnect security domains owned by the same mobile operator (which is a possibility allowed by clause 4.4.1) then the Za-interface is not subject to roaming agreements as assumed by clause 5.5 and 5.6.2
Summary of change:	⌘	Clarify that roaming agreements are not always needed for Za-interface.
Consequences if not approved:	⌘	The Za-interface may misinterpreted as being only applicable to inter-operator communication and specification will stay inconsistent.

Clauses affected:	⌘	5.5 ; 5.6.2

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

⌘

Other comments: ⌘

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

5.5 Security policy granularity

The policy control granularity afforded by NDS/IP is determined by the degree of control with respect to the ESP Security Association between the NEs or SEGs. The normal mode of operation is that only one ESP Security Association is used between any two NEs or SEGs, and therefore the security policy will be identical to all secured traffic passing between the NEs.

This is consistent with the overall NDS/IP concept of security domains, which should have the same security policy in force for all traffic within the security domain. The actual inter-security domain policy is determined by roaming agreements when the security domains belong to different operators or may be unilaterally decided by the operator when the security domains both belong to him. IPsec security policy enforcement for inter-security domain communication is a matter for the SEGs of the communicating security domains.

*****next 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. The SEGs use IKE to negotiate, establish and maintain a secure ESP tunnel between them. ~~Subject to roaming agreements, I~~inter-SEG tunnels can~~would normally~~ 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.

  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~~all roaming partners~~. 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 ~~is~~ 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 ~~for roaming partners~~ 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.

3GPP TSG-SA3#27 ***Tdoc ⌘S3-030128***
Sophia Antipolis, France, 25-28 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.210** **CR** **006** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Za-interface and roaming agreements
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	26/2/2003
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:	⌘	In case two SEG's interconnect security domains owned by the same mobile operator (which is a possibility allowed by clause 4.4.1) then the Za-interface is not subject to roaming agreements as assumed by clause 5.5 and 5.6.2
Summary of change:	⌘	Clarify that roaming agreements are not always needed for Za-interface.
Consequences if not approved:	⌘	The Za-interface may misinterpreted as being only applicable to inter-operator communication and specification will stay inconsistent.

Clauses affected:	⌘	5.5 ; 5.6.2

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

⌘

Other comments: ⌘

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

5.5 Security policy granularity

The policy control granularity afforded by NDS/IP is determined by the degree of control with respect to the ESP Security Association between the NEs or SEGs. The normal mode of operation is that only one ESP Security Association is used between any two NEs or SEGs, and therefore the security policy will be identical to all secured traffic passing between the NEs.

This is consistent with the overall NDS/IP concept of security domains, which should have the same security policy in force for all traffic within the security domain. The actual inter-security domain policy is determined by roaming agreements when the security domains belong to different operators or may be unilaterally decided by the operator when the security domains both belong to him. IPsec security policy enforcement for inter-security domain communication is a matter for the SEGs of the communicating security domains.

*****next 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. The SEGs use IKE to negotiate, establish and maintain a secure ESP tunnel between them. ~~Subject to roaming agreements, I~~inter-SEG tunnels can~~would normally~~ 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.

  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~~all roaming partners~~. 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 ~~is~~ 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 ~~for roaming partners~~ 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.