Technical Specification Group Services and System Aspects **TSGS#19(03)0105**

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

Source: **SA WG3**

Title: **2 CRs to 33.210: Clarification to the re-keying aspects of network domain security (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-030105	33.210	007	-	Rel-5	Clarification to the re-keying aspects of network domain security	F	5.2.0	SEC-NDS-IP	S3-030162
SP-030105	33.210	008	-	Rel-6	Clarification to the re-keying aspects of network domain security	A	6.0.0	SEC-NDS-IP	S3-030163

3GPP TSG-SA3 Meeting #27
Sophia Antipolis, France, 25-28th February 2003

Tdoc ⌘S3-030162

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **007** ⌘ **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:	⌘	Clarification to the re-keying aspects of network domain security
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	12/02/2003
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:	⌘	The procedures for handling the lifetime and rekeying of security associations are not currently clearly specificied in any IETF standards.
Summary of change:	⌘	The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires
Consequences if not approved:	⌘	Procedures for re-keying of security associations will be unclear. SEGs deemed interoperable would be prone to drop packets when re-keying unless these requirements are clarified. Configuration of SEGs could become too complex unless these specifications are clarified.

Clauses affected:	⌘	5.4

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

⌘

Other comments:	⌘	

First modified section

5.4 Profiling of IKE

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following additional requirement on IKE is made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported;
- Only Main Mode shall be used;
- Only Fully Qualified Domain Names (FQDN) shall be used;
- Support of 3DES in CBC mode shall be mandatory for confidentiality;
- Support of SHA-1 shall be mandatory for integrity/message authentication.

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires. The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data being transmitted within the old SA.

For IKE phase-2 (IPsec SA):

- Perfect Forward Secrecy is optional;
- Only IP addresses or subnet identity types shall be mandatory address types;
- Support of Notifications shall be mandatory.

3GPP TSG-SA3 Meeting #27
Sophia Antipolis, France, 25-28th February 2003

Tdoc ⌘S3-030163

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **008** ⌘**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 **X**

Title:	⌘	Clarification to the re-keying aspects of network domain security
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	12/02/2003
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:	⌘	The procedures for handling the lifetime and rekeying of security associations are not currently clearly specificied in any IETF standards.
Summary of change:	⌘	The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires
Consequences if not approved:	⌘	Procedures for re-keying of security associations will be unclear. SEGs deemed interoperable would be prone to drop packets when re-keying unless these requirements are clarified. Configuration of SEGs could become too complex unless these specifications are clarified.

Clauses affected:	⌘	5.4

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

Other comments: ⌘

First modified section

5.4 Profiling of IKE

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following additional requirement on IKE is made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported;
- Only Main Mode shall be used;
- Only Fully Qualified Domain Names (FQDN) shall be used;
- Support of 3DES in CBC mode shall be mandatory for confidentiality;
- Support of SHA-1 shall be mandatory for integrity/message authentication.

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires. The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data being transmitted within the old SA.

For IKE phase-2 (IPsec SA):

- Perfect Forward Secrecy is optional;
- Only IP addresses or subnet identity types shall be mandatory address types;
- Support of Notifications shall be mandatory.