Technical Specification Group Services and System Aspects **TSGS#21(03)0488**

Meeting #21, Frankfurt, Germany, 22-25 September 2003

Source: **SA WG3**

Title: **2 CRs to 33.210: Change of IKE profiling (Rel-5 & Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meet	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SAWG3 Doc
SP-21	SP-030488	33.210	011	-	Rel-5	F	Change of IKE profiling	5.4.0	5.5.0	S3-030350
SP-21	SP-030488	33.210	012	-	Rel-6	A	Change of IKE profiling	6.2.0	6.3.0	S3-030354

3GPP TSG-SA3 Meeting #29
San Francisco, USA, July 15-19, 2003

Tdoc ⌘S3-030350

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **011** ⌘**rev** **-** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Change of IKE profiling
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	04/07/2003
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:	⌘	1. Current IKE profiling imposes undue requirements on interconnect networks. 2. Mandatory DNS support forces operators to introduce undesired vulnerability potential into the NDS/IP environment.
Summary of change:	⌘	IP addresses are also allowed as IKE peer identification.
Consequences if not approved:	⌘	NDS/IP does not work in inter-domain networks without a common DNS hierarchy.

Clauses affected:	⌘	5.4

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

Other comments:	⌘	

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~~ IP addresses and Fully Qualified Domain Names (FQDN) shall be ~~used~~supported for identification;
- 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 #29
San Francisco, USA, July 15-19, 2003

Tdoc ⌘[H1]S3-030354

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **012** ⌘**rev** **-** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Change of IKE profiling
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	07/07/2003
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:	⌘	1. Current IKE profiling imposes undue requirements on interconnect networks. 2. Mandatory DNS support forces operators to introduce undesired vulnerability potential into the NDS/IP environment.
Summary of change:	⌘	IP addresses are also allowed as IKE peer identification.
Consequences if not approved:	⌘	NDS/IP does not work in inter-domain networks without a common DNS hierarchy.

Clauses affected:	⌘	5.4

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

Other comments: ⌘

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~~ IP addresses and Fully Qualified Domain Names (FQDN) shall be ~~used~~supported for identification;
- 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.