TSGS#24(04)0374

Source: **SA WG3 (Security)**

Title: **CR to33.210: Diffie-Hellman groups in NDS/IP (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-0400374	33.210	016	-	Rel-6	Diffie-Hellman groups in NDS/IP	F	6.4.0	S3-040291	SEC-NDS-IP

3GPP TSG-SA WG3 Security #33
Beijing, China, 10 –14 May 2004

Tdoc ⌘S3-040291

CR-Form-v7

CHANGE REQUEST

⌘ **33.210** **CR** **016** ⌘**rev** **-** ⌘ Current version: **6.4.0** ⌘

*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 **X**

Title:	⌘	Diffie-Hellman groups in NDS/IP
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	28/04/2004
Category:	⌘	**F**
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 Diffie-Hellman (DH) Groups are needed for the entropy of key generation by the DH exchange. There are two types of DH Groups; MODP (Modular Exponential) and EC2N (Elliptic Curves). The general rule when choosing suitable DH group is to think about the needed security of the keys - the larger modulus, the larger entropy of the keys generated by the DH exchange.

DH1 is the 768-bit MODP group. This can be thought too weak when speaking about today's encryption functions. Its usage can be justified only in rare, special cases. The minimum recommendation for chosen DH group is the DH2 with 1024-bit MODP. DH5 group is 1536-bit MODP. It is another more secure choice in addition to the DH2.

DH3 and DH4 groups are elliptic curves (EC) and based on the Galois Field GF[2^155], GF[2^185], respectively. These two groups seem to have some vulnerable characteristics based on comments of some EC cryptographers.

IETF has also discussed about the stronger DH groups and they have introduced remarkably bigger groups (MODP >3000-bit) but they are not used so widely at the moment in the industry. Also the handling of the bigger groups is slower compared to smaller ones.

NDS/IP does not explicitly specify required DH group. IKE (RFC 2409) requires support only for weak DH1 and recommends support for DH2.

Summary of change: ⌘ The change introduces mandatory support for DH2

Consequences if ⌘ IKE will use DH1 in key generation and keys may not be strong enough

not approved:	

Clauses affected:	⌘	5.4			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

********** Change **********

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;
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;
- Support of 3DES in CBC mode shall be mandatory for confidentiality;
- Support of AES in CBC mode (RFC-3602 [29]) shall be mandatory for confidentiality;
- Support of SHA-1 shall be mandatory for integrity/message authentication;
- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

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;
- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

Key Length and support of AES transform:

Since the AES-CBC allows variable key lengths, the Key Length attribute must be specified in both a Phase 1 exchange [20] and a Phase 2 exchange [18]. It is noted that the key length for use with this specification shall be 128 bits.