3GPP TSG SA WG3 Security — S3#22 **S3-020080**

25 - 28 February 2002

Bristol, UK

Source: **Nokia**

Title: **Proposed Changes to 33.210 about the ISAKMP SA**

Document for: **Discussion/Decision**

Agenda Item: **x.x**

There are two distinct Security Associations: ISAKMP (IKE Phase I) and IPsec (IKE Phase II). The section 5.4 of the 33.210 specification contains already the following:

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

This contribution proposes clarification to the definition of SAs. The changes are edited with change marks against 33.210 v1.1.0.

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Anti-replay protection: Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographical integrity mechanism in place.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

NDS/IP Traffic: Traffic that requires protection according to the mechanisms defined in this specification.

Security Association: A bi-directional or unidirectional logical connection created for security purposes. All traffic traversing a~~n~~ ~~IPsec~~ SA is provided the same security protection. The ~~IPsec~~ SA itself is set of parameters to define ~~a unidirectional~~ security protection between two entities. A~~n IPsec~~ Security Association includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

Security Domain: Networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical.

Transport mode: Mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers.

Tunnel mode: Mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
BG	Border Gateway
CS	Circuit Switched
CSCF	Call State Control Function
DES	Data Encryption Standard
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload
GTP	GPRS Tunnelling Protocols
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security - a collection of protocols and algorithms for IP security incl. key mngt.
ISAKMP	Internet Security Association Key Management Protocols
IV	Initialisation Vector
MAC	Message Authentication Code
NAT	Network Address Translator
NDS	Network Domain Security
NDS/IP	NDS for IP based protocols
NE	Network Entity
PS	Packet Switched
SA	Security Association
SAD	Security Association Database (sometimes also referred to as SADB)
SEG	Security Gateway
SIP	Session Initiation Protocol
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
TrGW	Transition Gateway

5.1 Security services afforded to the protocols

IPsec offers a set of security services, which is determined by the negotiated IPsec security associations. That is, the IPsec SA defines which security protocol to be used, the ~~SA~~ mode and the endpoints of the SA.

In the UMTS NDS the IPsec security protocol shall always be ESP and the ~~SA~~ mode shall always be tunnel mode. In NDS it is further mandated that integrity protection/message authentication together with anti-replay protection shall always be used.

The security services provided by NDS/IP:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional);
- limited protection against traffic flow analysis when confidentiality is applied;

5.2 Security Associations (SAs)

In the UMTS network domain security architecture the key management and distribution between SEGs is handled by the protocol Internet Key Exchange (IKE) (RFC-2407 [18], RFC-2408 [19] and RFC-2409 [20]). The main purpose of IKE is to negotiate, establish and maintain Security Associations between parties that are to establish secure connections. The concept of a Security Association is central to IPsec and IKE.

To secure typical, bi-directional communication between two hosts, or between two security gateways, an ISAKMP Security Association and two IPsec Security Associations (one in each direction) are required.

IPsec Security associations are uniquely defined by the following parameters:

- A Security Parameter Index (SPI)
- An IP Destination Address (this is the address of the ESP SA endpoint)
- A security protocol identifier (this will always be the ESP protocol in NDS/IP)

With regard to the use of IPsec security associations in the UMTS network domain control plane the following is noted:

- NDS/IP only requires support for tunnel mode IPsec SAs
- NDS/IP only requires support for ESP IPsec SAs
- There is no need to be able to negotiate IPsec SA bundles since a single ESP SA is sufficient to set up to protect traffic between the nodes

The ~~IPsec~~ specification of IPsec SAs can be found in RFC-2401 [12].

ISAKMP Security associations are uniquely defined by the following parameters:

- Initiator's cookie
- Responder's cookie

With regard to the use of ISAKMP security associations in the UMTS network domain control plane the following is noted:

- NDS/IP only requires support for ISAKMP SAs with pre-shared keys

The specification of ISAKMP SAs can be found in RFC-2408 [19].

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 AES 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 lif~~t~~etime for at least the same duration as does the derived IPsec SAs.

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

NOTE: When AES MAC is defined for IKE by the IETF it will also be made mandatory for IKE phase-1 in NDS/IP.

Editor’s Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.