ERICSSON

S3z010076
(S3-010335)
(postponed
S3-010221)

MAPSEC DOI Version -02

A presentation in the 3GPP SA3 meeting #18 in Phoenix, Arizona, May 2001.

Jari Arkko

Ericsson

Status

- As of 07 am monday morning, a –02 version exists ;-)
- Includes Siemens comments to Madrid
- Includes Madrid agreements
- Includes Alcatel comments

Modifications (1)

- Main Mode has been mandated.
- SA deletion has become mandatory.
- Rules for assigning new numbers within this DOI have been clarified.
- It has also been made clear which numbers are defined in this document (such as the attribute numbers) and which ones are defined in the 3GPP Technical Specifications (such as the protection profile numbers).
- KINK is no longer referenced in this document.
- ISAKMP protocol and transform identifiers have been removed.
- MAPSEC transform, Authentication, Algorithm, and Protection Profile values have been left to be defined by 3GPP Technical Specifications.

Modifications (2)

- References have been completed.
- The format of the PLMN Id has been specified.
- There are no longer private use value space for attribute values.
- The size of the protection profile entity has been specified to be 16 bit.
- No longer copy the key derivation text from IKE, reference instead.
- Port and protocol fields in the Identity payload have been mandated to be always zero.
- No longer describe the network architectures other than pointing to the 3GPP specifications (and noting that other archictures are also possible).

ERICSSON

New Network Architecture Text

The MAP Security protocol and its key management part provides authentication, confidentiality, integrity, and replay protection services to the MAP messages it transports.

The purpose of the MAP Security header in the protocol is to provide enough information to determine the MAP SA and Protection Modes used in securing the MAP operation that follows the header.

MAPSEC DOI and IKE are used to set up Security Associations for nodes implementing MAPSEC. While the MAP protocol usually runs over SS7, the MAPSEC DOI and IKE are always run over IP. It is therefore assumed that nodes or networks implementing MAPSEC always have IP connectivity in addition to the SS7 connectivity.

The network architectures where the MAPSEC DOI can be run include but are not limited to the one defined by 3GPP [NDSEC]. In the 3GPP architecture the MAPSEC is typically run between two different network operators, and the same SAs are shared by a number NEs.

It is possible that the nodes using MAPSEC DOI and IKE also have some other, IP traffic to protect. The MAPSEC DOI allows a single Phase 1 IKE to be used for the negotiation of both MAP and IP traffic protection using different Phase 2 exchanges and DOI identifiers.

As in IKE, the MAPSEC DOI allows only symmetric Security associations to be set up. That is, a pair of SAs is always created for the incoming and outgoing directions. These SAs differ only with respect to the keys, SPIs, and peer identities but all other parameters including the algorithms will have the same values.

Modifications (3)

- The use of several key lengths in the context of e.g. AES has been clarified
- Section 4.3 has been replaced by a brief policy comments
- References to the IPSEC DOI, ISAKMP, and IKE requirements have been clarified to be relevant for Phase 1 only in section 3.5 and 4.6.2

ERICSSON

Open Issues

- One unclear comment from Siemens regarding the Situation field
- Alcatel asked for the possibility to provide only integrity, and only confidentiality
- At a future time, we may need to specify somewhere else how to do certificate management for MAPSEC
- Text in TS 33.200 A.2 necessary?
- SA definition in TS 33.200 C.1 in right place?
- Must move the text fragments from DoI to 33.200

Move text #1, MAPSEC_AES

MAPSEC_AES 2

The MAPSEC_AES type specifies a generic MAP Security transform using AES. The actual protection suite is determined in concert with an associated authentication algorithm and other SA parameters.

The MAPSEC_AES transform is defined in ???.

All implementations MUST use the MAPSEC DOI Key Length attribute in concert with this transform in order to specify the desired key length for use with AES. All implementations MUST support at least the key length 128, and MAY support key lengths 192 and 256.

Move text #2, AES_CBC_MAC

AES-CBC-MAC 5

The semantics of the AES-CBC-MAC are defined in ???.