3GPP TSG SA WG3 Security — S3#21 **S3-010695**

27 - 30 November, 2001

Sophia Antipolis, France

Source:	Siemens Atea
Title:	Mapping of Ze-interface information onto the Zd-Interface.
Document for:	Discussion / Decision
Agenda item:	MAP security Rel-5

1) References from MAPDoI Version 4 [S3-0100615] to TS 33.200 Rel-5[NDS]

3.2. Domains of Interpretation:

In chapter 4, this document defines all Phase 2 related issues for the MAPSEC DOI. In addition, 3GPP Technical Specifications [NDSEC] specify the actual MAPSEC authentication and encryption algorithms, as well as so called protection profiles. At the same time, [NDSEC] defines the values that are used in the MAPSEC DOI to refer to these algorithms and profiles. This ensures that the MAPSEC DOI document does not have to be modified upon the development of a new authentication algorithm, for instance.

4.1 Naming Scheme

Within ISAKMP, all DOI's MUST be registered with the IANA in the "Assigned Numbers" RFC [STD-2]. The IANA Assigned Number for the MAP Security DOI (MAPSEC DOI) is TBD (N). Within the MAP Security DOI, all well-known identifiers MUST be registered with the IANA under the MAPSEC DOI. Unless otherwise noted, all tables within this document refer to IANA Assigned Numbers for the MAPSEC DOI. See Section 6 for further information relating to the IANA registry for the MAPSEC DOI. The MAPSEC DOI also makes use of several numbers defined by the 3GPP Technical Specification [NDSEC].

4.4.2 MAPSEC Transform Identifiers (Subchapter of 4.4 MAPSEC Assigned Numbers)

The following table lists the reserved MAPSEC Transform Identifiers.

Transform ID	Value
RESERVED	0-1

Actual MAP Transform Identifiers are defined in the 3GPP Technical Specification [NDSEC].

4.5 MAPSEC Security Association Attributes

Authentication Algorithm

RESERVED 0-4

This specification only lists the reserved values. **Actual Authentication Algorithm values are defined in the 3GPP Technical Specification [NDSEC].**

There is no default value for Authentication Algorithm, as it must be specified to correctly identify the applicable transform.

Implementor's note: The first five values are reserved by the IPSEC DOI.

Key Length

RESERVED 0

There is no default value for Key Length, as it must be specified for transforms using ciphers with variable key lengths. For fixed length ciphers, the Key Length attribute MUST NOT be sent. **The definition of MAPSEC transforms in the 3GPP Technical Specifications such as [NDSEC] MUST specify if the use of Key Length is necessary and what the legal values are.**

2) Proposed text to be included in TS 33.200 Rel-5 based on S3-010608 (without change bars).

5.6 MAPsec algorithms

5.6.1 Mapping of MAP-SA encryption algorithm identifiers

The MEA algorithm indication fields in the MAP-SA are used to identify the encryption algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below. The KAC will assign the MAP Encryption Algorithm Identifier onto the MAPsec DoI TransformID [7] when negotiating a new pair of MAPsec-SA.
The KAC shall use the Key Length Attribute of the SA for IKE phase 2 as this information is implicitly available for the Partner KAC via the used TransFormID.

Table 1: MAP encryption algorithm identifiers

MAP Encryption Algorithm identifier	Description
0	Null
1	AES in a stream cipher mode (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 Description of MEA-1

The MEA-1 algorithm is the ISO/IEC 10116 Counter Mode with parameter j=128 bits, SV=IV and truncation of the last block is according to the method described in ISO/IEC 10116 Annex A.5.3. See ISO/IEC 10116 [5] for more information.

Editor's Note: More specification on the mode of operation for MEA-1 may be required.

5.6.2 Mapping of MAP-SA integrity algorithm identifiers

The MIA algorithm indication fields in the MAP-SA are used to identify the integrity algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.
The KAC shall assign the MAP Integrity Algorithm Identifier onto the authentication algorithm attribute of the SA [7] for IKE phase 2 when negotiating a new pair of MAPsec-SA.

Table 2: MAP integrity algorithm identifiers

MAP Integrity Algorithm identifier	Description
0	Null
1	AES in a CBC MAC mode with a 128-bit key (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.2.1 Description of MIA-1

The MIA-1 algorithm is the ISO/IEC 9797 Part 1: padding method 2, MAC algorithm 1 (initial transformation=1, output transformation=1). No IV used. The MAC-length m is 32-bits (see clause 5.6.1). See ISO/IEC 9797 [6] for more information.

3) Remaining Questions

A) Exact Mapping of MIA to authentication algorithm as 5 values have been reserved by Ipsec DoI already.
B) Exact Mapping of MEA to TransformID as 2 values have been reserved already.
C) How exactly shall the KAC use the parameter Key Rounds.