3GPP TSG SA WG3 Security — S3#20 **S3-010693**

27 - 30 November, 2001

Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** ⌘ ev **-** ⌘ Current version: **4.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Completing the specification of a MAPsec SA
Source:	⌘	Hutchison 3G UK
Work item code:	⌘	MAPsec
Date:	⌘	22-11-01
Category:	⌘	**F**
Release:	⌘	Rel-4

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)

Reason for change:	⌘	To explicitly complete the specification of a MAPsec SA and make it clear that since destination PLMN-Id and SPI uniquely determine an SA, they should belong to that SA.
Summary of change:	⌘	Adding Destination PLMN-Id, SPI and Sending PLMN-Id to an SA.
Consequences if not approved:	⌘	The specification of an SA will be incomplete and it will be left unclear if the elements that uniquely determine an SA actually belong to that SA. The change ensures SAs can be **uniquely identified** in the SAD and avoids the possibility of incompatible implementations.

Clauses affected:	⌘	5.4
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

5.4 MAPsec security association attribute definition

The MAPsec security association shall contain the following data elements:

- **Destination PLMN-Id:**

  PLMN-Id is the ID number of the receiving Public Land Mobile Network (PLMN). The value for the PLMN-Id is a concatenation of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the receiving network.

- **Security Parameters Index (SPI):**

  SPI is a 32-bit value that is used in combination with Destination PLMN-Id to uniquely identify a MAP-SA.

- **Sending PLMN-Id:**

  PLMN-Id is the ID number of the sending Public Land Mobile Network (PLMN). The value for the PLMN-Id is a concatenation of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the sending network.

- **MAP Encryption Algorithm identifier (MEA):**

  Identifies the encryption algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in clause 5.6.

- **MAP Encryption Key (MEK):**

  Contains the encryption key. Length is defined according to the algorithm identifier.

- **MAP Integrity Algorithm identifier (MIA):**

  Identifies the integrity algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in section 5.6.

- **MAP Integrity Key (MIK):**

  Contains the integrity key. Length is defined according to the algorithm identifier.

- **Protection Profile Identifier (PPI):**

  Identifies the protection profile. Length is 16 bits. Mapping of profile identifiers is defined in section 6.

- **SA Lifetime:**

  Defines the actual expiry time of the SA. The expiry of the lifetime shall be given in UTC time.

Editor's Note: The exact format and length to be defined.

A MAPsec SA is uniquely identified by a destination PLMN-Id and a Security Parameters Index, SPI. As a consequence, during SA creation, the SPI is always chosen by the receiving side.

If the SA is to indicate that MAPsec is not to be applied then all the algorithm attributes shall contain a NULL value.