3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010086**

13 September, 2001, Sophia Antipolis, France

CR-Form-v3

CHANGE REQUEST

⌘ **33.200** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*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 ☒

Title:	⌘	Correction to security policy requirements
Source:	⌘	Siemens AG
Work item code:	⌘	MAPsec
Date:	⌘	5 September 2001
Category:	⌘	**F**
Release:	⌘	Rel-4

Use one of the following categories:
- ***F*** *(essential 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:	⌘	*If proposed security policy requirements are not fulfilled, PLMNs implementing MAP security may remain vulnerable against active attacks even if all other operators support MAP security as well.*
Summary of change:	⌘	Implement request by SA#10, resolve editorial note on section 5.3 “Policy requirements for the MAPsec SPD”, introduce clarifications in section 6
Consequences if not approved:	⌘	Reduced security level for MAP security

Clauses affected:	⌘	Sections 4, 5.3, 6.2, 6.3, Annex A.2		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	tba
Other comments:	⌘			

4 Principles of MAP application layer security

This technical specification defines mechanisms for protecting the MAP protocol at the application layer. The MAP protocol may also be protected at the network layer when IP is used as the transport protocol. However, whenever inter-working with networks using SS7-based transport is necessary, protection at the application layer shall be used.

The security measures specified in this TS are only fully useful if all interconnected operators use them. In order to prevent active attacks all interconnected operators must at least use MAPsec with the suitable protection levels as indicated in this specification and treat the reception of all MAP messages (protected and unprotected) in a uniform way in the receiving direction. Additionally this requires the introduction of a cut-off date for this feature, which is to be agreed among operators

Before protection can be applied, Security Associations (SA) needs to be established between the respective MAP network elements. Security associations define, among other things, which keys, algorithms, and protection profiles to use to protect MAP signalling. The necessary MAP-SAs between networks are negotiated between the respective network operators. The negotiated SA will be effective PLMN-wide and distributed to all network elements which implement MAP application layer security within the PLMN. Signalling traffic protected at the application layer will, for routing purposes, be indistinguishable from unprotected traffic to all parties except for the sending and receiving entities.

Protection at the application layer implies changes to the application protocol itself to allow for the necessary security functionality to be added.

The MAP application layer security interface between MAP-NEs engaged in security protected signalling is referred to in this specification as the Zf interface. The interface applies to all MAPsec transactions, intra- or inter-PLMN.

5.3 Policy requirements for the MAPsec Security Policy Database (SPD)

The security policies for MAPsec key management are specified in the NE's SPD. SPD entries define which MAP operation components are protected and which MAP SAs (if any) to use to protect MAP signalling based on the PLMN of the peer NE. There can be no local security policy definitions for individual NEs. Instead, SPD entries of different NE within the same PLMN shall be identical.

Fallback to unprotected mode.

- Procedures to set the "~~information about the possiblity to allow~~ fallback to unprotected mode" (enabled/disabled) in the MAP-NEs must be provided. For the receiving direction, it is sufficient to have a single parameter indicating whether fallback for incoming messages is allowed or not. For the sending direction, the information should indicate for each destination PLMN -whether fallback for outgoing messages is allowed or not. This state~~information~~ shall~~must~~ be available to the MAP-NE before any communication towards other MAP-NEs can take place.

- The use of the fallback indicators is specified in Annex B.

- The security measures specified in this TS are only fully useful for a particular PLMN if it disallows fallback to unprotected mode for MAP received from any other PLMN after a certain cut-off date.

Table of MAPsec operation components

- The security policy database (SPD) may optionally contain a table of MAPsec operation components for incoming messages. MAPsec operation components are operation components which have to be carried in a MAPsec message. i.e. with a MAP security header. The use of this table is specified in Annex B.

~~Editor's note: More text on processing of incoming MAP messages needed.~~

Uniformity of protection profiles

- In order to ensure full protection, a particular PLMN shall use the same protection profile for incoming MAPsec messages from all other PLMNs. In particular, full protection is not ensured when protection profile A (no protection) is used for some source PLMNs and other profiles are used for other source PLMNs.

Editor's note: Some issues need to be investigated: ~~Include and clarify fallback indicator~~; Policy for SA renewal, the need for START time, mechanism to distinguish inbound/outbound SPDs ? ~~Implications of Protection Mode 0 differing between operators for the same type of operation (Danger of active attacker changing the source PLMN ID).~~

6.2 MAPsec protection groups

This section specifies groups of messages and their protection modes at the operation component level. Individual protection groups or particular combinations of groups can then be used to construct protection profiles as specified in section 6.3.It is recommended to only use the protection groups defined here.

Combinations of overlapping protection groups are forbidden. Forbidden combinations are explicitly specified in 6.2.1 below.

The concept of "protection levels" is introduced to administrate the protection mode on operation component level. A protection level of an operation determines the protection modes used for the operation's components according to the following table.

Table 3: MAPsec protection levels

Protection level	Protection mode for *invoke* component	Protection mode for *result* component	Protection mode for *error* component
1	1	0	0
2	1	1	0
3	1	2	0
4	2	1	0
5	2	2	0
6	2	0	0

6.2.1 MAPsec protection groups

6.2.1.1 MAP-PG(0) – No Protection

This MAP-PP does not contain any operation and it does not protect any information. It is useful however to have a "null" MAP-PP to use in situations where no security is required or is an option. This protection group cannot be combined with any other protection group.

6.2.1.2 MAP-PG(1) – Protection for Reset

Table 4: PG(1) – Protection for Reset

Application Context/Operation	Protection Level
ResetContext-v2/ Reset	1
ResetContext-v1/ Reset	1

6.2.1.3 MAP-PG(2) – Protection for Authentication Information except Handover Situations

Table 5: PG(2) – Protection for Authentication Information except Handover Situations

Application Context/Operation	Protection Level
InfoRetrievalContext-v3/ Send Authentication Info	3
InfoRetrievalContext-v2/ Send Authentication Info	3
InfoRetrievalContext-v1/ Send Parameters	3
InterVlrInfoRetrievalContext-v3/ Send Identification	3
InterVlrInfoRetrievalContext-v2/ Send Identification	3

6.2.1.4 MAP-PG(3) – Protection for Authentication Information in Handover Situations

Table 6: PG(3) – Protection for Authentication Information in Handover Situations

Application Context/Operation	Protection Level (Component level)
HandoverControlContext-v3/ Prepare Handover (Note that the AC contains also other operations)	4
HandoverControlContext-v3/ Forward Access Signalling (Note that the AC contains also other operations)	4
HandoverControlContext-v2/ Prepare Handover (Note that the AC contains also other operations)	4
HandoverControlContext-v2/ Forward Access Signalling (Note that the AC contains also other operations)	4
HandoverControlContext-v1/ Perform Handover (Note that the AC contains also other operations)	4
HandoverControlContext-v1/ Forward Access Signalling (Note that the AC contains also other operations)	4

6.2.1.5 MAP-PG(4) – Protection of non location dependant HLR data

Table 7: PG(4) – Protection of non location dependant HLR data

Application Context/Operation	Protection Level
AnyTimInfoHandlingContext-v3 / AnyTimeModification	1
SubscriberDataMngtContext-v3 / DeleteSubsciberData	1

Editor's Note: Protection Group 4 is not complete.

6.3 MAPsec protection profiles

Protection profiles can be individual protection groups or particular combinations of protection groups. MAP protection profiles are coded as a 16 bit binary number where each bit corresponds to a protection group. Currently only 5 groups are defined, the rest are reserved for future use.

Table 8: Protection profile encoding

Protection profile bit	Protection group
0	No protection
1	Reset
2	Authentication information except handover situations
3	Authentication information in handover situations
4	Non-location dependant HLR data
5-15	Reserved

It is recommended to only use the protection profiles defined here.

Protection profiles are by definition bidirectional.

The following protection profiles are defined.

Table 9: Protection profile definition

Protection profile name	**Protection group**				
	PG(0) *No protection*	PG(1) *Reset*	PG(2) *AuthInfo except handover situations*	PG(3) *AuthInfo in handover situation*	PG(4) *Non-location dependant HLR data*
Profile A	✓				
Profile B		✓	✓		
Profile C		✓	✓	✓	
Profile D		✓	✓	✓	✓
Profile E		✓	✓		✓

A.2 Local Security Association Distribution

Manual Local Security Association Distribution is executed entirely within one PLMN and is consequently at the discretion of the administrative authority.

The requirement on the manual distribution procedures can be summarized as follows:

~~- Fallback to unprotected mode. MAPsec may be **required** or it may be **optional** towards other MAP-NEs. Procedures to set this information in the MAP-NEs on a per PLMN destination basis must be provided. This information should available to the MAP-NE before any communication towards other MAP-NEs is to take place. MAP-NEs capable of executing MAPsec should define a default value for the MAPsec **fallback to unprotected mode** indicator.~~

    - Procedures for transporting the relevant MAPsec SA to the MAP-NEs must be defined. In order to ensure that the MAPsec SA are present when needed, all valid MAPsec SA should be distributed to all MAP-NEs as soon as they are available.

- Procedures for revocation of MAPsec SAs must be defined