Technical Specification Group Services and System Aspects
Meeting #14, Kyoto, Japan, 17-20 December 2001

TSGS#14(01)0617

Source: **SA WG3**

Title: **4 CRs to 33.200: Related to Protection Profiles (Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
33.200	013		Rel-4	F	Use of 'Original component identifier' during MAPsec processing	4.1.0	4.2.0	S3-010471
33.200	014		Rel-4	F	Protection Profiles correction	4.1.0	4.2.0	S3-010541
33.200	015		Rel-4	F	Policy configuration clarification	4.1.0	4.2.0	S3-010542
33.200	018		Rel-4	F	Protection Profile Revision Identifier	4.1.0	4.2.0	S3-010691

3GPP TSG SA WG3 Security — S3#20 **S3-010471**

16-19 October 2001, Sidney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **013** ⌘ 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 ☒

Title:	⌘	Use of 'Original component identifier' during MAPsec processing
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-MAP
Date:	⌘	08-10-2001
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:	⌘	1) Annex B on 'MAPsec message flows' does not specify how the 'Original Component Identifier' of the received MAPsec message is used to select the Protection Profile that was applied to the message. A MAPsec NE receiving an inbound message must evaluate the 'Original Component Identifier' field to be able to determine the protection level applied to the MAPsec message. Without knowing the protection level, it is not possible to "apply" an SA to a MAPsec message, as it is not clear whether integrity only, integrity and encryption or no protection has to be applied. 2) Editorial change in 1.c
Summary of change:	⌘	Clarification on how the 'Original Component Identifier' has to be used for MAPsec message processing in MAPsec.
Consequences if not approved:	⌘	Incomplete MAPsec inbound message processing.

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

Annex B (Normative): MAPsec message flows

Imagine a network scenario with two MAP-NEs at different PLMNs (NEa and NEb) willing to communicate using MAPsec. Figure 1 presents the message flow.

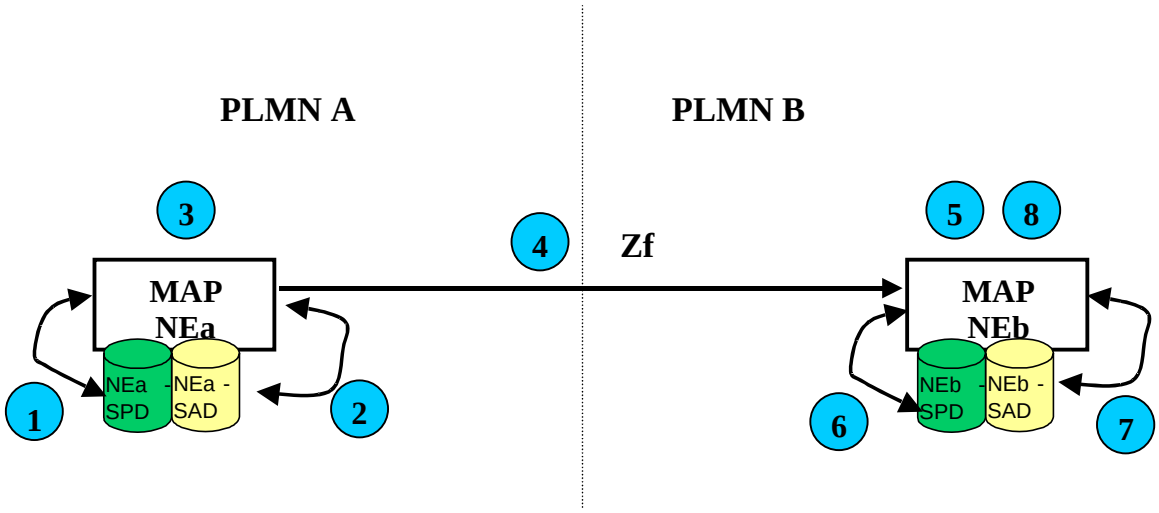

Figure 1. MAPsec Message Flow

According to Figure 1, when MAP-NEa (NEa) from PLMN A wishes to communicate with a MAP-NEb (NEb) of PLMN B using MAP protocol, the process is the following:

As the Sending Entity, NEa performs the following actions during the outbound processing of every MAP message:

1. NEa checks its Security Policy Database (SPD) to check if MAP security mechanisms shall be applied towards PLMN B:

   a) If the SPD does not mandate the use of MAPsec towards PLMN B, then normal MAP communication procedures will be used and the process continues in step 4.b.

   b) If the SPD mandates the use of MAPsec towards PLMN B, then the process continues at step 2.

   c) If no valid entry in the SPD is found for PLMN B, then the communication is aborted and an error is returned to the MAP user.

2. NEa checks its Security Association Database (SAD) for a valid Security Association (SA) to be used towards PLMN B. In the case where more than one valid SA is available at the SAD, NEa shall choose the one expiring the sooner.

a) In case protection of MAP messages towards PLMN B is not possible (e.g. no SA available, invalid SA…), then the communication is aborted and an error is returned to MAP user.

b) If a valid SA exists but the MAP dialogue being handled does not require protection (Protection Mode 0 applies to all the components of the dialogue), then either the original MAP message in cleartext is sent in step 4.b, or a MAPsec message with Protection Mode 0 is created in step 3.

c) If a valid SA exists and the MAP dialogue being handled requires protection, then the process continues at step 3.

3. NEa constructs the MAPsec message towards NEb using the parameters (keys, algorithms and protection profiles) found in the SA.

4. NEa generates either:

   a) MAPsec message towards NEb.

   b) An unprotected MAP message in the event that the SPD towards NEb or protection profiles for that specific MAP dialogue so allows it (1.a. or 2.b.).

At the Receiving Entity, NEb performs the following actions during the inbound processing of every MAP message it received:

5. If an unprotected MAP message is received, the process continues with step 6.

   Otherwise, NEb decomposes the received MAPsec message and retrieves basic information to apply security measures (‘SPI’, ‘sending PLMN-ID’, ‘TVP’, ‘IV’ and ‘Original Component Identifier’).

   Freshness of the protected message is checked at this time. If the Time Variant Parameter (TVP) received in the protected message is out of the acceptable window then the message shall be discarded and an error is returned to MAP user. No error message is returned to NEa.

6. NEb checks the SPD:

   An unprotected MAP message is received:

   a) If an unprotected MAP message is received and fallback to unprotected mode is allowed, then the unprotected MAP message is simply processed (Process goes to END)

   b) If an unprotected MAP message is received and the ‘MAPsec operation components table’ of the SPD does not mandate the use of MAPsec for the included ‘Original Component Identifier’, then the unprotected MAP message is simply processed (Process goes to END)

   c) If an unprotected MAP message is received, the ‘MAPsec operation components table’ of the SPD mandates the use of MAPsec for the included ‘Original Component Identifier’ and fallback to unprotected mode is NOT allowed, then the message is discarded.

      If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

   A MAPsec message is received:

   d) If no valid entry in the SPD is found for PLMN A, then the message is discarded and an error is reported to MAP user.

      If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

e) If a MAPsec message is received, but the SPD indicates that MAPsec is NOT to be used, then the message is discarded and an error is reported to MAP user.

If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

f) If a MAPsec message is received and the SPD indicates that MAPsec is required, then the process continues at step 7.

7. NEb checks its SAD to retrieve the relevant SA-information for processing of the MAPsec message:

a) If the received SPI points to a valid SA, then NEb uses the 'Original Component Identifier' in the MAPsec header to identify the protection level that has to be applied to the component indicated, according to the protection profile indicated in the SA. Tthe process continues at step 8.

b) If the received SPI does not point to a valid SA, the message is discarded and an error is reported to MAP user. If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

8. Integrity and encryption mechanisms are applied ~~on~~ to the message according to the identified protection level, by using the information in the SA (Keys, algorithms~~, protection profiles~~).

a) If the result after applying such mechanisms is NOT successful then the message is discarded and an error is reported to MAP user. If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

b) If the result after applying such procedures is successful, then NEb has the cleartext MAP message NEa originally wanted to send NEb. The cleartext MAP message can now be processed (Process goes to END)

END: A cleartext MAP message is available at NEb.

In the event the received message at NEb requires an answer to NEa (Return Result/Error), NEb will perform the process in steps 1 to 4 acting as the Sender and NEa will perform the process in steps 5 to 8 acting as the Receiver.

In the event a MAPsec enabled NE initiated a secured MAP communication towards a non-MAPsec enabled NE and the MAPsec enabled NE received an error indication of such circumstance (i.e. "ApplicationContextNotSupported"). The MAPsec enabled NE shall check whether "Fallback to Unprotected Mode" is allowed:

- If NOT allowed, then the communication is aborted.
- If allowed, then the MAPsec enabled NE shall send an unprotected MAP message instead.

The same procedures shall apply to secure MAP communications between MAP-NEs in the same PLMN.

NOTE: Because various error cases may be caused by active attacks, it is highly recommended that the cases are reported to the management system.

3GPP TSG SA WG3 Security — S3#20 **S3-010541**

16-19 October 2001, Sidney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **014** ⌘ 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:	⌘	Protection Profiles correction
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-MAP
Date:	⌘	08 oct 2001
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:	⌘	Correction to MAP-PG(4) – Protection of non location dependant HLR data This group contains the ApplicationContext : "SubscriberDataMngtContext-v3/ DeleteSubscriberData", that does not change HLR data, but VLR-data. Additionally, this ApplicationContext does not provide a risk.
Summary of change:	⌘	Remove the applicationContext 'SubscriberDataMngtContext-v3/ DeleteSubscriberData' from the protection profiles. Editors note is removed as no further critical application contexts were identified related to non-location dependant HLR data
Consequences if not approved:	⌘	MAP-PG(4) specification is left inconsistent, and the editors note can not be removed.

Clauses affected:	⌘	6.2.1.5
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

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
AnyTimeInfoHandlingContext-v3 / AnyTimeModification	1
~~SubscriberDataMngtContext-v3 / DeleteSubsciberData~~	~~1~~

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

3GPP TSG SA WG3 Security — S3#20 **S3-010542**

16 - 19 October, 2001

Sydney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **015** ⌘ 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 ☒

Title:	⌘	Policy configuration clarification
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-MAP
Date:	⌘	09 Oct 2001
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:	⌘	A good security practise requires the explicit inclusion of all communication partners (PLMN's) in the policy database. Within Annex B (Flows) it was already described that, when a MAPsec message is received and no valid entry in the SPD is found for PLMN A, then the message is discarded and an error is reported to MAP user.
Summary of change:	⌘	Explicit configuration requirement for the SPD is included in relevant clause 5.3.
Consequences if not approved:	⌘	Network operators not aware of this may experience MAPsec network introduction problems.

Clauses affected:	⌘	5.3
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications
	⌘	
Other comments:	⌘	

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:

- The "fallback to unprotected mode" (enabled/disabled) shall be available to the MAP-NE before any communication towards other MAP-NEs can take place. 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;

- 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 messages received from any other PLMN.

Table of MAPsec operation components:

- The security policy database (SPD) shall contain a table of MAPsec operation components for incoming messages. This table contains operation components which have to be carried in MAPsec messages with Protection Mode 1 or 2. The use of MAPsec operation components is specified in Annex B.

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.

Explicit policy configuration:

- The SPD shall contain an entry for each PLMN the MAP-NE is allowed to communicate with.

Editor's note: Some issues need to be investigated: Non-synchronised expiration times issue, mechanism to distinguish inbound/outbound SPDs ?

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **018** ⌘ 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:	⌘	Protection Profile Revision Identifier
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-MAP
Date:	⌘	29 November 2001
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 overcome current inflexibility in the concept of the MAP-PG and PPI assignments that forces to define new MAP-PG for each new change that adds/deletes existing AC to/from existing Protection Profiles.
Summary of change:	⌘	Add a 1 byte identifier to define Protection Profiles revisions.
Consequences if not approved:	⌘	The reserved MAP-PG bits will exhaust and extra bits may be required in future anyhow. This will cause changes to former 3GPP releases at the time of bits exhaustion. The rationale of grouping Application Contexts together that belong functionally together in the same MAP-PG cannot be followed.

Clauses affected:	⌘	3.3; 5.4; 6.3
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

****** First Modification ******

3.3 Abbreviations

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

AES	Advanced Encryption Standard
FALLBACK	Fallback to unprotected mode indicator
IP	Internet Protocol
IV	Initialisation Vector
MEK	MAP Encryption Key
MAC	Message Authentication Code
MAC-M	MAC used for MAP
MAP	Mobile Application Part
MAP-NE	MAP Network Element
MAPsec	MAP security – the MAP security protocol suite
MEA	MAP Encryption Algorithm identifier
MIA	MAP Integrity Algorithm identifier
MIK	MAP Integrity Key
NDS	Network Domain Security
NE	Network Entity
PPI	Protection Profile Indicator
PPRI	Protection Profile Revision Identifier
PROP	Proprietary field
SA	Security Association
SADB	Security Association DataBase
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
TVP	Time Variant Parameter

****** Second Modification ******

5.4 MAPsec security association attribute definition

The MAPsec security association shall contain the following data elements:

- **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 Revision Identifier (PPRI):**

  Contains the revision number of the PPI. Length is 8 bits. PPRI-values are defined in section 6.3

- **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.

****** Next Modification ******

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. The protection that shall be applied to a MAPsec message is uniquely identified by the combination of PPRI and PPI.

This specification contains the MAPsec protection profiles that are identified with PPRI having value 0. 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

Protection profiles shall be 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		✓	✓		✓