3GPP TSG-SA WG3 Meeting #17 ***S3-010087***
Göteborg, Sweden, 27 February-2 March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **33.200** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **0.3.2** ⌘

*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:	⌘	MAP Protection Profiles
Source:	⌘	Siemens
Work item code:	⌘	Network Domain Security
Date:	⌘	27-Feb-01
Category:	⌘	**D**
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:	⌘	Include MAP protection profiles in 33.200.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.2.7, Annex B.1		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

7.2.7 MAPsec protection profiles

MAPsec specifies a set of protection profiles. These profiles specifies the required protection level per MAP operation. The protection profile is then a set of attribute pairs (operation, protection level). Annex B.1 contains definitions for standard MAPsec protection profiles.

Table 3: Example of (Operation, Protection level) attribute pairs

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)
AuthenticationFailureReport	1 (authenticity/integrity)
CheckImei	1 (authenticity/integrity)

The protection level for a specified operation applies for the operation irrespective of the dialogue/application context that the operation is part of. Corollary, a dialogue/application context may contain operations with different protection level. All components in a protected operation shall be protected with the same protection level.

NOTE: Operations shall have the same protection level for both the request and the response phase.

B.1 ~~UMTS Security~~Protection Profiles for MAPsec

A MAP Protection Profile (MAP-PP) is an attribute in a MAPsec Security Association. A MAP-PP defines for every MAP dialogue (identified by the application context and the first operation) whether protection is required. If so, it defines for every operation within this dialogue the protection level to be used. The protection level of an operation within a protected dialogue defines ~~the operations that shall be protected and~~ the applied protection modes for every component (invoke, result, error) of the operation according to the following table:

protection level	protection mode for invoke component	protection mode for result component	protection mode for error component
0	0	0	0
1	1	1	1
2	2	2	2
3	1	0	0
4	0	1	0
5	0	0	1
6	2	0	0
7	0	2	0
8	0	0	2
9	1	1	0
10	1	0	1
11	0	1	1
12	1	1	2
13	1	2	1
14	2	1	1
15	2	2	0
16	2	0	2
17	0	2	2
18	2	2	1
19	2	1	2
20	1	2	2
21	0	1	2
22	0	2	1

23	1	0	2
24	1	2	0
25	2	0	1
26	2	1	0

The following table defines the standardized MAP-PPs:

Application contect	Operation	Protection level					
		PP(0)	PP(1)	PP(2)	PP(3)	PP(4)	PP(5) ffs
infoRetrieval-v1	Send Parameters	-	-	-	24	9	
infoRetrieval-v2	Send Authentication Info	-	-	-	24	9	
infoRetrieval-v3	Send Authentication Info	-	24	9	24	9	
interVlrInfoRetrieval-v2	Send Identification	-	-	-	24	9	
interVlrInfoRetrieval-v3	Send Identification	-	24	9	24	9	
anyTimeInfoHandling-v3	Any Time Modification	-	24	9	24	9	
	Any Time Subscription Interrogation	-	24	9	24	9	
anyTimeInfoEnquiry-v3	Any Time Interrogation	-	24	9	24	9	
reset-v1	Reset	-	-	-	3	3	
reset-v2	Reset	-	-	-	3	3	
all other ACs	and operations	-	-	-	-	-	

.

MAP-PP(0): No Protection

This MAP-PP does not contain any dialogue~~operation~~ and it does not protect any information. This MAP-PP is used when no security is required or no security is an accepted option.

~~Operation~~	~~Protection Mode~~

MAP-PP(1): Protection for UMTS Authentication Information and HLR-SCP signalling traffic (a)

This MAP-PP protects

- UMTS Authentication information (quintets) with confidentiality,
- request for UMTS Authentication information (quintets) with authenticity/integrity,
- interrogation and modification requests from the SCP to the HLR with authenticity/integrity,
- interrogation and modification responses from the HLR to the SCP with confidentiality

~~in other than handover situations. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:~~

~~Operation~~	~~Protection Mode~~
~~Send Authentication Info~~	~~2~~
~~Send Parameters (only if requested parameterList includes requestAuthenticationSet)~~	~~2~~
~~Send Identification~~	~~2~~

~~Additionally, MAP-PP(1) proposes to protect the following critical MAP operation:~~

~~Operation~~	~~Protection Mode~~
~~Reset~~	~~1~~

~~The rest of MAP dialogues carrying operations not included in this list are considered not to be protected.~~

MAP-PP(2): Protection for UMTS Authentication Information and HLR-SCP signalling traffic (b)~~including Handover Situations~~

This MAP-PP protects

- UMTS Authentication information (quintets) with authenticity/integrity,
- request for UMTS Authentication information (quintets) with authenticity/integrity,
- interrogation and modification requests from the SCP to the HLR with authenticity/integrity,
- interrogation and modification responses from the HLR to the SCP with authenticity/integrity

~~This MAP-PP will protect Authentication information in all situations. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:~~

~~Operation~~	~~Protection Mode~~
~~Send Authentication Info~~	~~2~~
~~Send Parameters (only if requested parameterList includes requestAuthenticationSet)~~	~~2~~
~~Send Identification~~	~~2~~
~~Prepare Handover~~	~~2~~
~~Perform Handover~~	~~2~~
~~Forward Access Signalling~~	~~2~~

~~Additionally, MAP-PP(2) proposes to protect the following critical MAP operation:~~

~~Operation~~	~~Protection Mode~~
~~Reset~~	~~1~~

~~The rest of MAP dialogues carrying operations not included in this list are considered not to be protected.~~

MAP-PP(3): Protection for Authentication, ~~and Location Information~~ HLR-SCP signalling traffic and reset messages (a)

This MAP-PP protects

- UMTS and GSM Authentication information (quintets and triplets) with confidentiality,
- request for UMTS and GSM Authentication information (quintets and triplets) with authenticity/integrity,
- interrogation and modification requests from the SCP to the HLR with authenticity/integrity,
- interrogation and modification responses from the HLR to the SCP with confidentiality,
- reset messages with authentication/integrity

~~This MAP-PP will protect Authentication and Location information. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:~~

~~Operation~~	~~Protection Mode~~

~~Send Authentication Info~~	~~2~~
~~Send Parameters (only if requested parameterList includes requestAuthenticationSet)~~	~~2~~
~~Send Identification~~	~~2~~
~~Prepare Handover~~	~~2~~
~~Perform Handover~~	~~2~~
~~Forward Access Signalling~~	~~2~~
~~Update Location~~	~~2~~
~~Update GPRS Location~~	~~2~~
~~Prepare Subsequent Handover~~	~~2~~
~~Perform Subsequent Handover~~	~~2~~
~~Provide Subscriber Info~~	~~2~~

~~Additionally, MAP-PP(3) proposes to protect the following critical MAP operation:~~

~~Operation~~	~~Protection Mode~~
~~Reset~~	~~1~~

~~The rest of MAP dialogues carrying operations not included in this list are considered not to be protected.~~

~~[Editor: It seems unwise to proceed with the MAPsec profiles before we have a clear idea of what the MAPsec DoI RFC will contain.]~~

MAP-PP(4): Protection for Authentication, HLR-SCP signalling traffic and reset messages (b)

This MAP-PP protects

- UMTS and GSM Authentication information (quintets and triplets) with authenticity/integrity,
- request for UMTS and GSM Authentication information (quintets and triplets) with authenticity/integrity,
- interrogation and modification requests from the SCP to the HLR with authenticity/integrity,
- interrogation and modification responses from the HLR to the SCP with authenticity/integrity,
- reset messages with authentication/integrity

MAP-PP(5): FFS