**3GPP TSG SA WG3 Security — S3#20** **S3-010493**

**16-19 October 2001, Sydney, Australia**

*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:*** | ⌘ | Flexible Protection Profiles for MAP |
| ***Source:*** | ⌘ | Hutchison 3G UK |
| ***Work item code:*** | ⌘ | Security |
| ***Date:*** | ⌘ | 11 October 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:*** | ⌘ | Allow flexibility in MAPsec security to deal with unforeseen security weaknesses. |
| ***Summary of change:*** | ⌘ | Standardises the protection profiles that can be used in a propriertary manner and adds protection groups to cover all messages. |
| ***Consequences if not approved:*** | ⌘ | MAPsec does not have the flexibility to cover future security threats. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.2, 6.3 |
| ***Other specs affected:*** | ⌘ | ☐ Other core specifications ⌘<br>☐ Test specifications<br>☐ O&M Specifications |
| ***Other comments:*** | ⌘ | |

## 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.

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/<br>Reset | 1 |
| ResetContext-v1/<br>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.

### 6.2.1.6 MAP-PG(13) – Integrity Protect other messages

This MAP-PP contains all MAP operations not specified in another group of a profile and applies protection level 2 to them all.

**Table 8: PG(13) – Protect all messages**

| Application Context/Operation | Protection Level |
|---|---|
| All MAP operations not in other groups | 2 |

### 6.2.1.7 MAP-PG(14) – Full protection

This MAP-PP contains all MAP operations and applies protection level 5 to them all. This protection group cannot be combined with any other protection group.

**Table 9: PG(14) – Protect all messages**

| Application Context/Operation | Protection Level |
|---|---|
| All MAP operations | 5 |

## 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 7~~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 |
| 5-12~~5~~ | Reserved |
| 13 | Integrity protect remaining messages |
| 14 | Protect al messages |
| 15 | Proprietary profile flag |

Protection profiles shall be bidirectional. Proprietary protection profiles must be implemented.

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 | | ✓ | ✓ | | ✓ |