

---

# 3GPP TS 33.200 V0.7.6.0 (2001-05)

*Technical Specification*

**3rd Generation Partnership Project;  
Technical Specification Group SA3  
3G Security;  
Network Domain Security;  
MAP application layer security  
(Release 4)**



The present document has been developed within the 3<sup>rd</sup> Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

---

Keywords

---

Security, Core Network, MAP, Key management

**3GPP**

Postal address

---

3GPP support office address

---

650 Route des Lucioles - Sophia Antipolis  
Valbonne - FRANCE  
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

---

<http://www.3gpp.org>

---

**Copyright Notification**

---

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2000, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).  
All rights reserved.

---

# Contents

|   |                      |
|---|----------------------|
| Foreword.....   | 4                    |
| Introduction.....   | 4                    |
| 1 Scope .....   | 5                    |
| 2 References .....  | 5                    |
| 3 Definitions, symbols and abbreviations.....   | 5                    |
| 3.1 Definitions .....   | 5                    |
| 3.2 Symbols.....  | 6                    |
| 3.3 Abbreviations .....   | 6                    |
| 4 Principles of MAP application layer security.....   | 6                    |
| 5 MAP security (MAPsec) .....   | 7                    |
| 5.1 Security services provided by MAPsec .....  | 7                    |
| 5.2 Properties and tasks of MAPsec enabled network elements.....                            | 7                    |
| 5.3 MAPsec security association attribute definition .....                                  | 7                    |
| 5.3.3 Policy requirements for the MAPsec SPD .....  | 8                    |
| 5.4 MAPsec structure of protected messages .....  | 8                    |
| 5.4.1 MAPsec protection modes .....   | 8                    |
| 5.4.2 Protection Mode 0.....  | 9                    |
| 5.4.3 Protection Mode 1.....  | <a href="#">109</a>  |
| 5.4.4 Protection Mode 2.....  | <a href="#">109</a>  |
| 5.5 MAPsec security header .....  | <a href="#">109</a>  |
| 5.6 MAPsec algorithms .....   | <a href="#">1140</a> |
| 5.6.1 Mapping of MAP-SA algorithm identifiers .....   | <a href="#">1140</a> |
| 5.6.2 Construction of IV .....  | <a href="#">1140</a> |
| 6 MAPsec protection profiles .....  | 12                   |
| 6.1 Granularity of protection .....   | 12                   |
| 6.2 MAPsec protection groups .....  | 12                   |
| 6.2.1 MAPsec protection groups.....   | 12                   |
| 6.2.1.1 MAP-PG(0) – No Protection .....   | 12                   |
| 6.2.1.2 MAP-PG(1) – Protection for Reset.....   | 12                   |
| 6.2.3 MAP-PG(2) – Protection for Authentication Information except Handover Situations..... | 13                   |
| 6.2.1.4 MAP-PG(3) – Protection for Authentication Information in Handover Situations .....  | 13                   |
| 6.2.1.6 MAP-PG(4) – Protection of non location dependant HLR data .....                     | 13                   |
| 6.2 MAPsec protection profiles .....  | 14                   |
| <b>Annex A (informative): Guidelines for manual key management .....</b>                    | <b>15</b>            |
| A.1 Inter-domain Security Association and Key Management Procedures (Zd-interface).....     | 15                   |
| A.2 Local Security Association Distribution (Ze-interface) .....                            | 15                   |
| <b>Annex B (informative): Change history.....</b>   | <b>15</b>            |

---

## Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

## Introduction

The absence of security in SS7 networks is an identified security weakness in 2G systems. This was formerly perceived not to be a problem, since the SS7 networks were the provinces of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

For 3G systems it is a clear goal to be able to protect the core network signalling protocols, and by implication this means that security solutions must be found for both SS7 and IP based protocols.

Various protocols and interfaces are used for control plane signalling to/from, inside and between core networks. The security services that have been identified as being needed are confidentiality, integrity, authentication and anti-replay protection. These will be ensured by standard procedures, based on cryptographic techniques.

---

# 1 Scope

This technical specification covers the security mechanisms and procedures necessary to protect the MAP protocol. The complete set of enhancements and extensions to facilitate security protection for the MAP protocol is termed MAPsec and it covers transport security in the MAP protocol itself and the security management procedures.

The security mechanisms specified for MAP are on the application layer. This means that MAPsec is independent of the network and transport protocols to be used.

This technical specification contains the stage-2 specification for security protection of the MAP protocol. The actual implementation (stage-3) specification can be found in the MAP stage-3 specification, TS 29.002 [4].

This specification applies to MAP version 3, TS 29.002 [4] Rel-4 and higher.

NOTE: It is explicitly noted that the automated key management and key distribution parts of MAPsec is not part of Rel-4. All key management and key distribution in Rel-4 must therefore be carried out by other means. (See Annex A.)

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- [1] 3G TS 21.133: Security Threats and Requirements
- [2] 3G TS 21.905: 3G Vocabulary
- [3] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- [4] 3G TS 29.002: Mobile Application Part (MAP) specification

---

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

**Anti-replay protection:** Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographic integrity mechanism in place.

**Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

**Data integrity:** The property that data has not been altered in an unauthorised manner.

**Data origin authentication:** The corroboration that the source of data received is as claimed.

**Entity authentication:** The provision of assurance of the claimed identity of an entity.

**Key freshness:** A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

**Security Association:** A logical connection created for security purposes. All traffic traversing a security association is provided the same security protection. The security association specifies protection levels, algorithms to be used, lifetime of the connection etc.

**MAPsec:** The complete collection of protocols and procedures needed to protect MAP messages. MAPsec can be divided into three main parts. These are (1) MAPsec transport security, (2) MAPsec Local Security Association distribution and (3) MAPsec Inter-domain Security Association and Key Management procedures.

## 3.2 Symbols

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

Zf                    The MAPsec-MAP application layer security interface between networks/security domains for secure-MAP-NEs interoperation engaged in security protected signalling.

## 3.3 Abbreviations

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

|        |  |
|--------|--|
| AES    | Advanced Encryption Standard                                       |
| IP     | Internet Protocol  |
| IV     | Initialisation Vector  |
| MAC    | Message Authentication Code  |
| MAP    | Mobile Application Part  |
| MAP-NE | MAP Network Element  |
| MAPsec | MAP security – the MAP security protocol suite                     |
| NDS    | Network Domain Security  |
| NE     | Network Entity   |
| SA     | Security Association   |
| SADB   | Security Association Database (sometimes also referred to as SADB) |
| SPD    | Security Policy Database (sometimes also referred to as SPDB)      |
| SPI    | Security Parameters Index  |
| TVP    | Time Variant Parameter   |

## 3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

---

# 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.

Before protection can be applied, Security Associations (SA) need 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.

A central concept introduced in this technical specification is the notion of a security domain. Within a security domain the same level of security and usage of security services is applied. For MAP application layer security, only one security domain shall exist per PLMN.

Editors Note: This needs to be reformulated to indicate that security policies are set up between pairs.

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-security domain PLMN.

---

## 5 MAP security (MAPsec)

### 5.1 Security services provided by MAPsec

The security services provided by MAPsec are:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional).

### 5.2 Properties and tasks of MAPsec enabled network elements

MAPsec MAP-NEs shall maintain the following databases:

- NE-SPD-MAP: A database in an NE containing MAP security policy information (see clause 5.3);
- NE-SADB-MAP: A database in an NE containing MAP-SA information. MAP-NEs shall monitor the SA lifetime and expired SAs shall be deleted from the database (see clause 5.4).

MAPsec MAP-NEs shall be able to perform the following operations:

- Secure MAP signalling (i.e. send/receive protected or unprotected messages) according to information in NE-SPD-MAP and NE-SADB-MAP. The structure of protected messages is defined in clause 5.5 and the protection algorithms are defined in clause 5.6.

Editor's Note: Need to add flows from old Annex A.

### 5.3 Policy requirements for the MAPsec SPD

The security policies for MAPsec key management are specified in the NE's SPD. SPD entries define 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.

### 5.43 MAPsec security association attribute definition

The MAPsec security association is a sequence of the following data elements:

*MAPsec security association = EAI // EK // IAI // IK // PPI // Fallback // SA lifetime*

The following MAP security association attributes are defined:

- **Encryption Algorithm Identifier (EAI):**

Identifies the encryption algorithm. Length is four bits. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in section 5.6.

Editor's Note: — Format to be defined..

- **Encryption Key (EK):**

Contains the encryption key. Length is 128 bits.

~~Editor's Note: — Format to be defined.~~

- **Integrity Algorithm Identifier (IAI):**

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

~~Editor's Note: — Format to be defined.~~

- **Integrity Key (IK):**

Contains the integrity key. Length is 128 bits.

~~Editor's Note: — Format to be defined.~~

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

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

~~Editor's Note: — Format to be defined.~~

- **Fallback to Unprotected Mode Indicator (Fallback):**

In the case that protection is available, this parameter indicates whether fallback to unprotected mode is allowed. This is a one bit indicator where the value one indicates that fall back to unprotected mode is permitted and value zero indicates that fallback to unprotected mode is not permitted.

~~Editor's Note: — Format to be defined.~~

- **SA Lifetime:**

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

*Editor's Note: Format and length to be defined.*

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

### ~~5.3.1 Policy requirements for the MAPsec SPD~~

The security policies for MAPsec key management are specified in the NE's SPD. SPD entries define 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.

~~Editors Note: Need to add a table to define the SPD entries, include/clarify Fallback allowed indicator. Policy for SA renewal needed SA\_Start, etc. Need to include separate SPDs for inbound and Outbound.~~

## 5.45 MAPsec structure of protected messages

~~Editors NOTE: Security header defined before protected payload, then protection modes 5.4.1–5.5–5.4.2~~

### ~~5.4.1 MAPsec protection modes~~

MAPsec provides for three different protection modes and these are defined as follows:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity



Protection Mode 2: Confidentiality, Integrity, and Authenticity

MAP operations protected by means of MAPsec consists of a Security Header and the Protected Payload. Secured MAP messages have the following structure:

|                 |                   |
|-----------------|-------------------|
| Security Header | Protected Payload |
|-----------------|-------------------|

In all three protection modes, the security header is transmitted in cleartext.

In protection mode 2 providing confidentiality, the protected payload is essentially the encrypted payload of the original MAP message (see chapter 5.4.4). For integrity and authenticity in protection modes 1 and 2, the message authentication code is calculated on the security header and the payload of the original MAP message in cleartext and it is included in the protected payload. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP message.

### 5.5.1 MAPsec security header

The security header is a sequence of the following data elements:

*Security header = TVP // NE-Id // Prop // Sending PLMN-Id // SPI // Original component Id*

- **TVP:**

The TVP is used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived is 0.1 seconds. The size of the time-window at the receiving network entity is not standardised.

- **NE-Id:**

6 octets used to create different IV values for different NEs within the same TVP period. It is necessary and sufficient that NE-Id is unique per PLMN. (This is sufficient because sending keys are unique per PLMN.) The NE-Id shall be the global title of the NE without the MCC and MNC.

- **Proprietary field (Prop):**

4 octet used to create different IV values for different protected MAP messages within the same TVP period for one NE. The usage of the proprietary field is not standardised.

- **Sending PLMN-Id:**

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

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

SPI is an arbitrary 32-bit value that is used in combination with the sender's PLMN-Id to uniquely identify a MAP-SA.

- **Original Component identifier:**

Identifies the type of component within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).

Editor's Note: It may be necessary to have some way of distinguishing direction (intra-PLMN case).

### 5.5.2 Protected payload

#### 5.5.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload of Secured MAP messages in protection mode 0 is identical to the original MAP message payload in cleartext.

For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP message. ~~It is therefore allowed as an implementation option to let Protection Mode 0 operations be sent without the security header.~~

#### ~~5.4.35.2.2~~ Protection Mode 1

The protected payload of Secured MAP messages in protection mode 1 takes the following form:

|   |
|---|
| Cleartext   H(Security Header  Cleartext) |
|---|

where "Cleartext" is the payload of the original MAP operation in clear-text. Therefore, in Protection Mode 1 the protected payload is a concatenation of the following information elements:

- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity key defined by the security association to the concatenation of Security Header and Cleartext. The MAC length shall be 32 bits.

~~Editor's Note: — Length of the MAC needs to be defined.~~

#### ~~5.4.45.2.3~~ Protection Mode 2

The protected payload of Secured MAP Messages in protection mode 2 takes the following form:

|   |
|---|
| E( Cleartext)    H(Security Header   E( Cleartext)) |
|---|

where "Cleartext" is the original MAP message payload in clear-text. Confidentiality is achieved by encrypting Cleartext using the encryption function E with the confidentiality key defined by the security association. Authentication of origin and integrity are achieved by applying the message authentication code (MAC) function H with the integrity key defined by the security association to the concatenation of Security Header and encrypted Cleartext. The MAC length shall be 32 bits.

~~Editor's Note: — Length of the MAC needs to be defined.~~

### ~~5.5~~ ~~MAPsec security header~~

~~The security header is a sequence of the following data elements:~~

~~□ Transmitted IV (IV<sub>T</sub>):~~

~~□ TVP:~~

~~The TVP is used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived is 0.1 seconds. The size of the time-window at the receiving network entity is not standardised.~~

~~□ NE-Id:~~

~~6 octets used to create different IV values for different NEs within the same TVP period. It is necessary and sufficient that NE-Id is unique per PLMN. (This is sufficient because sending keys are unique per PLMN.)~~

~~Editor's Note: — The scheme for allocating or calculating the NE-Id is to be defined.~~

~~□ Proprietary field (Prop):~~

4 octet used to create different IV values for different protected MAP messages within the same TVP period for one NE. The usage of the proprietary field is not standardised.

**□ Sending PLMN-Id:**

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

**□ Security Parameter Index (SPI):**

SPI is an arbitrary 32-bit value that is used in combination with the sender's PLMNID to uniquely identify a MAP-SA.

**□ Original Component identifier:**

Identifies the type of component within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).

Editors Note: It may be necessary to have some way of distinguishing direction (intra-PLMN case)

## 5.6 MAPsec algorithms

### 5.6.1 Mapping of MAP-SA algorithm identifiers

The algorithm indication fields in the MAP-SA are used to identify the algorithms and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

**Table 3: MAPsec integrity algorithm identifiers**

| Integrity algorithm identifier | Description                       |
|--------------------------------|-----------------------------------|
| 0000                           | Null                              |
| 0001                           | AES in a CBC MAC mode (MANDATORY) |
| -not yet assigned-             | -not yet assigned-                |

Editor's Note: ~~Should a null algorithm be defined.~~

Editor's Note: More specification on the mode of operation is required.

**Table 4: MAPsec encryption algorithm identifiers**

| Encryption algorithm identifier | Description                             |
|---------------------------------|---|
| 0000                            | Null                                    |
| 0001                            | AES in a stream cipher mode (MANDATORY) |
| -not yet assigned-              | -not yet assigned-                      |

Editor's Note: ~~Should a null algorithm be defined.~~

Editor's Note: ~~More specification on the mode of operation is required.~~

### 5.6.2 Construction of IV

The IV used in the encryption shall be constructed as follows:

$$IV = TVP // NE-Id // Prop // Pad$$

The padding field is used to expand  $TVP // NE-Id // Prop$  to the IV length required by the cryptographic scheme in use.

Editor's Note: Padding rules to be defined.

## 6 MAPsec protection profiles

### 6.1 Granularity of protection

MAPsec protection is specified per MAP operation component.

### 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 5: MAPsec protection levels**

| Protection level | Protection mode for <i>invoke</i> component | Protection mode for <i>result</i> component | Protection mode for <i>error</i> 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

| Application Context/Operation | Protection Level |
|-------------------------------|------------------|
| ResetContext-v2/<br>Reset     | 1                |
| ResetContext-v1/<br>Reset     | 1                |

## 6.2.3 MAP-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

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

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

| Application Context/Operation                         | Protection Level |
|---|------------------|
| AnyTimInfoHandlingContext-v3<br>/ AnyTimeModification | 1                |

**Editor's NOTE:** Note: This protection group is incomplete (e.g. DeleteSubscriberData is missing).

## 6.2 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.

| 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  |

**Table 11: Protection profile encoding**

The following protection profiles are defined.

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

**Table 12: Protection profile definition**

Editor's note: Profiles B and C are different to those specified in the Siemens contribution S3-010192.

---

## Annex A (informative): Guidelines for manual key management

---

### A.1 Inter-domain Security Association and Key Management Procedures (Zd-interface)

Manual Inter-domain Security Association and Key Management procedures is subject to roaming agreements.

Some important parts of an inter-domain Security Association and Key Management agreement is:

- to defined how to carry out the initial exchange of MAPsec SAs
- to defined how to renew the MAPsec SAs
- to define how to withdraw MAPsec SAs (including requirements on how fast to execute the withdrawal)
- to decide if fallback to unprotected mode is to be allowed
- to decide on key lengths, algorithms, protection profiles, and SA lifetime etc (MAPsec SAs are expected to be fairly long lived)

---

### A.2 Local Security Association Distribution (Ze-interface)

Manual Local Security Association Distribution is executed entirely within one [security domain<sup>1</sup>PLMN](#) and is consequently at the discretion of the [security domain](#) administrative authority.

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

- 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 [security domainPLMN](#) destination basis must be provided. This information should be 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 **required/optional** parameter.
- 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

---

## Annex B (informative): Change history

| Change history |       |          |    |     |                 |     |     |  |
|----------------|-------|----------|----|-----|-----------------|-----|-----|--|
| Date           | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New |  |
|                |       |          |    |     |                 |     |     |  |
|                |       |          |    |     |                 |     |     |  |
|                |       |          |    |     |                 |     |     |  |

---

<sup>1</sup> Operators are expected define one security domain per network

~~Release 4 3GPP TS 33.200 V0.7.6.0 (2001-05) 3GPP TS 33.200 V0.7.6.0 (2001-05) 3GPP TS 33.200 V0.7.6.0 (2001-05) 3GPP TS 33.200 V0.6.0 (2001-05)~~

|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |