3GPP TSG SA WG3 Security — S3#18 **S3-010149**

21 - 24 May, 2001

Phoenix, USA

Source: **NDS Rapporteur**
Title: **Update information - TS 33.200**
Document for: **Information and Discussion**
Agenda Item: **9.2**

Update information

This document attempts to describe the main changes to TS33200 from v040 to v050.

It should be noted that the innocent sounding request from the S3#17bis NDS ad-hoc meeting to "remove the IP-only parts and move all MAPsec Rel5 material to an informative annex" in fact affects almost all of the TS.

That being so, I have had to reorganize and sometimes rewrite material in order for there to be any logical flow of information at all. (I don't quite now if I have succeeded)

The likelihood of me getting everything right in this version is rather small, and since the changes to the TS are pervasive and far reaching the interested parties are urged to carefully review TS33200 v050.

It must also be noted that there are still parts missing to the TS. In particular, the security algorithm interface description is **not** included. The to-do list, which we made at the meeting, should be found in the meeting report (which hopefully soon will be available on the server).

The following account only tries to explain the main changes made to the TS. There are numerous smaller changes. The table attempts to describe what v050 is like and how it differs from v040. Note that a number of IP-only sections from v040 are simply deleted.

/Geir M. Køien

Update information –TS 33.200

Section	Description
Title page	Title changed to "Network Domain Security; MAP application layer security"
Introduction	Some IP-only relevant material removed
1. Scope	Some IP-only relevant material removed
2. References	Only references that seems relevant are retained
3.1 Definitions	Slight change to **SA** definition. Definition of **MAPsec** attempted.
3.2 Symbols	Redundant symbols removed
3.3 Abbreviations	Redundant abbreviations removed
4. Overview…	Title modified to only cover SS7 based protocols
4.1 Introduction	IP-only material deleted
4.2 Protection…	New subsection. Material from old 4.1 restructured.
4.3 Security…	Contains material from old 4.2. Restructured.
4.4.1 Security…	Table-1/2 modified to only cover MAPsec needs
	Old section 5 moved to informative annex A
	Old section 6 deleted.
5 MAP security...	This section consists mainly of material from the old section 7.
5.2 Properties…	New. Taken from section 4.2 of S3z010005 (as agreed by S3#17bis)
5.3 MAPsec DoI	Restructured and simplified. A lot of this material is expected to be found either in the MAPsec DoI RFC or in our complementary MAPsec DoI definitions in normative annex C. (S3#17bis agreed to have a split of MAPsec DoI material in order to avoid frequent updating/replacements of the RFC) Push/pull (old 7.2.4) removed. Replacement found in Annex A. Protection profiles (old 7.2.7) removed. Replacement found in new section 6.
5.4 Structure…	Changed according to CR in S3z000032. (was section 7.2.5 in v040)
5.6 MAPsec…	Left as-is (old 7.2.8). Contribution required – Must be updated.
6 MAPsec prot…	New section. Material from S3z010033 (reply LS to CN4) as agreed by S3#17bis. Contains definitions for both operation and component level. Must be fixed to only one operation or component. S3 must await CN4 reply to this question. If CN4 has no comments, the default is operation.
Annex A	Old annex A deleted. New annex A contains MAPsec Rel5 material
A.1 Network…	Section on MAPsec architecture.
A.1.1 KACs	Section based on old 4.6. New material from section 4.1 of S3z010005 added.
A.1.2 UMTS…	Section closely based on old 5.4.
A.2 Inter-doma…	Not a lot of material here yet, but this is an informative annex on Rel5 matters so that shouldn't be a problem for Rel4. Material is needed for Rel5.
A.3 Local Secu…	Based entirely on S3z010005. Exception handling and recovery procedures are not part of this contribution, and some material covering these aspects is needed for Rel5.
	Old annex B on security profiles removed. See new section 6 for our brand new protection profiles which replaces old annex B.
Annex B	New annex. The rapporteur has taken the liberty to introduce this one. It is meant to cover the most basic needs for manual key mngt. The material included is meant just to kick off other contributions and shouldn't be taken as-is.
Annex C	Again a new annex. This annex is **normative** and is intended to cover: • MAPsec SA definitions • MAPsec DoI material that we don't want to be in the MAPsec DoI RFC

3GPP TS 33.200 V0.5.0 (2001-05)

Technical Specification

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

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

Contents

Foreword

This Technical Specification has been produced by the 3rd 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

An identified security weakness in 2G systems is the absence of security in SS7 networks. 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.

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 key management and distribution procedures. The key management interfaces and mechanisms are not part of Rel4, but an outline of the MAPsec key management and distribution architecture is included in annex A for information.

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, and MAPsec will therefore also apply should MAP be ported to IP based networks.

1 Scope

The scope of the UMTS network domain control plane is to cover the control signalling in the UMTS core network. This includes both the SS7 and IP based control plane signalling protocols. The present document defines the MAP security architecture for the UMTS network domain control plane.

The UMTS core network contains a number of SS7 based protocols, which in this specification are referred to as legacy protocols. While the stated goal of the network domain security is to cover all of the core network protocols, only MAP will be protected in Rel4. Behind this is a realization that SS7 based legacy protocols can in practice only be protected at the application layer, and that the work involved in protecting the legacy protocols therefore will be high and require redesign of the protocol itself. Even in the cases were it would be technically feasible to do the job it is questionable whether the benefits would ever justify the required effort. Consequently, the only legacy protocol that is protected in Rel4 is the MAP protocol [4].

NOTE-1: MAP inter-operator key management and local key distribution are part of Rel5.

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

[5] 3G TS 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[6] 3G TS 33.102: Security Architecture

[7] 3G TS 33.103: Security Integration Guidelines

[8] 3G TS 33.120: Security Objectives and Principles

[9] RFC-2401: Security Architecture for the Internet Protocol

[10] RFC-2406: IP Encapsulating Security Payload

[11] RFC-2407: The Internet IP Security Domain of Interpretation for ISAKMP

[12] RFC-2408: Internet Security Association and Key Management Protocol (ISAKMP)

[13] RFC-2409: The Internet Key Exchange (IKE)

[14] RFC-2412: The OAKLEY Key Determination Protocol

[15] draft-arkko-map-doi-01.txt: The MAP Security Domain of Interpretation for ISAKMP

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 cryptographical 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 an SA 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:

C	MAP interface between an HLR and an MSC
D	MAP interface between an HLR and a VLR
E	MAP interface between MSCs
Gc	Interface between a GGSN and an HLR
Gr	Interface between an SGSN and an HLR
Zd	MAPsec interface between KACs belonging to different networks/security domains
Ze	MAPsec interface between KACs and MAP-NEs within the same network
Zf	MAPsec interface between networks/security domains for secure MAP-NE interoperation.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security - a collection of protocols and algorithms for IP security incl. key mngt.
ISAKMP	Internet Security Association Key Management Protocols
IV	Initialisation Vector
KAC	Key Administration Centre
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
SAD	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

4 Overview over UMTS network domain security for SS7 based protocols

4.1 Introduction

The scope of this section is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains.

4.2 Protection at the application layer

If SS7 based protocols are to be protected they shall be protected at the application level. As the main rule, protocols that can be transported by either SS7 or IP networks shall be protected at the application layer. SS7 or mixed SS7/IP based protocols will commonly be referred to as legacy protocols in this specification.

For legacy protocols, the necessary security associations between networks are negotiated between Key Administration Centre entities. The negotiated SA will be effective network-wide and distributed to all affected network elements. 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. The network operator may have more than one KAC in its network in order to avoid a single point of failure or for performance reasons. A KAC may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

NOTE-1: It is explicitly noted that the automated key management and key distribution parts of MAPsec is not part of Rel4. All key management and key distribution in Rel4 must therefore be carried out by other means. (See Annex B)

4.3 Security for SS7 and mixed SS7/IP based protocols

As the general rule, legacy protocols shall be protected at the application layer. This implies changes to the application protocols themselves to allow for the necessary security functionality.

This 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]).

NOTE: It has been recognised that legacy protocols may also be protected at the network layer when using IP as the transport protocol. However, whenever interworking with networks using SS7-based transport is necessary then protection at the application layer shall be used.

4.4 Security domains

4.4.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. These control plane security domains may closely correspond to the core network of a single operator.

The specific network domain security interfaces for MAP is found in table 1. Annex-A contains a more detailed description of the Z-interfaces.

Table 1: Network domain security specific interfaces

Interface	Description	Network type
Zd	Network domain security interface between networks. The Zd-interface is defined for negotiation of MAP security associations between KACs.	IP
Ze	Network domain security interface between KAC and MAP-NE within the same network. The interface is security protected by means of an IPsec ESP tunnel.	IP
Zf	Network domain security interface between MAP-NEs engaged in security protected signalling (applies to MAP-NEs belonging to different or even to the same security domain)	SS7/MAP

The interfaces, which affects/is affected by this technical specification are described in the table below. Notice that when security protection is employed over an interface, this specification will refer to the Z-interface name.

NOTE: It is explicitly noted that only the Zf-interface is defined for Rel4. The Zd and Ze interfaces only apply to Rel5, but is included here for information.

Table 2: Interfaces that are affected by network domain security

Interface	Description	Affected protocol	Security implication
C	Interface between HLR and MSC	MAP	MAPsec shall be supported
D	Interface between HLR and VLR	MAP	MAPsec shall be supported
E	Interface between MSC and MSC	MAP	MAPsec shall be supported
G	Interface between VLR and VLR	MAP	MAPsec shall be supported
Gc	Optional interface between GGSN and HLR	MAP	MAPsec shall be supported
Gr	Interface between SGSN and HLR	MAP	MAPsec shall be supported

5 MAP security (MAPsec)

5.1 Security services afforded by MAPsec

The security services required for SS7 and mixed SS7/IP-based protocols 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 be able to perform the following operations:

- Request MAP-SA information to the KAC. This is done according to the “RequestSA” procedure outlined in Annex A.2
- Supervise MAP-SA lifetimes to initiate new valid SA information once the SA in use has expired. Optionally, the MAP-NE might request new SAs before the previous SAs have expired
- Secure MAP signalling (i.e. send/receive protected or unprotected messages) according to MAP-SA information received from the KAC

MAPsec MAP-NEs shall be responsible for the maintenance of the following databases:

- NE-SADB-MAP: A database in a NE containing MAP-SA information received from the KAC in the course of a "RequestSA" procedure. MAP-NEs shall control the SAs lifetime and the expired SAs shall be deleted of the database
- (Optional) NE-SADB-IP: Containing IPSec-SAs for protection of IP traffic between the KAC and NEs over the Ze interface

5.3 MAPsec Domain of Interpretation

Key management and distribution between operators for MAPsec is done by means of the Internet Key Exchange (IKE). To adapt IKE for use with MAPsec a MAPsec Domain of Interpretation (DoI) document is required. Such document is to defined and published within the IETF framework as a separate RFC. Currently the MAPsec DoI has the status of a draft RFC ([15]). Since the MAPsec DoI RFC is only concerned with non-IP issues it will be an informational RFC, but it shall nevertheless be normative for 3GPP MAPsec purposes.

5.3.1 MAPsec DoI requirements

ISAKMP (RFC-2408, [12]) places the following significant requirements on a DoI definition:

- Define the interpretation for the Situation field
- Define the set of applicable security policies
- Define the syntax for DoI-specific SA Attributes (Phase II)
- Define the syntax for DoI-specific payload contents
- Define additional Key Exchange types, if necessary
- Define additional Notification Message types, if needed

The normative MAPsec DoI definitions are found in the MAPsec DoI RFC ([15]). In addition to this Annex C contains complementary MAPsec definitions.

5.3.2 MAPsec Security Association Attributes

The following attributes are needed

- Protection Profile
- Authentication algorithm for integrity and authentication
- Encryption algorithm for confidentiality
- Encryption and authentication keys
- SA lifetime

5.3.3 Policy requirements for the MAPsec SPD

The policy is described as in the RFC-2401 [9] with following changes:

- The lifetime of the MAP SA is not defined as an amount of data transferred, but as absolute lifetime in seconds.
- The generated MAP SA will not be used for processing inbound and outbound traffic in KACs and thus processing choices *discard*, *bypass IPsec* and *apply IPsec* does not apply.
- The operator defines for which networks MAPsec SA's are negotiated.

The security policies for MAPsec key management are specified in the KACs' SPD by the network operator. The SPDs in the network elements are derived from the SPD of the KAC in the network. There can be no local security policy definitions for individual NEs.

5.4 MAPsec structure of protected messages

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 operation 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.

5.4.2 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.

5.4.3 Protection Mode 1

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

TVP||Cleartext|| H(TVP|| 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:

- Time Variant Parameter TVP
- 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 Time Variant Parameter TVP, Security Header and Cleartext.

The TVP used for replay protection of Secured MAP operations is a 32-bit time-stamp. The receiving network entity shall 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 must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

5.4.4 Protection Mode 2

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

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

where "Cleartext" is the original MAP message payload in clear text. Confidentiality is achieved by encrypting Cleartext 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 Time Variant Parameter TVP, Security Header and encrypted Cleartext.

The TVP used for replay protection of Secured MAP messages is a 32-bit time-stamp. The receiving network entity shall accept a message only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

It is recommended to use protection mode 2 whenever possible as this makes replay attacks even more difficult.

5.5 MAPsec security header

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

- **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.

- **Initialisation Vector (IV):**

  Initialisation vectors are used with block ciphers in chained mode to force an identical plaintext to encrypt to different cipher texts. Using IVs prevents launching a codebook attack against encrypted traffic. The IV has only local significance in the MAP-NE.

  NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.

- **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).

5.6 MAPsec algorithms

An algorithm indication field is used to identify the actual algorithms to be used. The MAPsec Integrity Algorithm (MIA) will be assigned to the MAPsec DoI TransformID.

Table 3: MAPsec Integrity Algorithm identifiers

MIA identifier	Description
00	Null
01	AES in CBC MAC mode (MANDATORY)
-not yet assigned-	-not yet assigned-

The MAPsec Encryption Algorithm (MEA) will be assigned to the MAPsec DoI TransformID

Table 4: MAPsec Encryption Algorithm identifiers

MEA identifier	Description
00	Null
01	AES (MANDATORY)
-not yet assigned-	-not yet assigned-

For both MIA and MEA the minimum key length shall be 128 bits.

6 MAPsec protection profiles

[EDITOR: The material in this section is almost entirely based on S3z010033 section 2. It is not intended to be the final word on this issue, but to provide a useful start for this section.

Note: This section describes both the operation level and component level options. The protection groups defined in this section are still under consideration in S3.]

6.1 Granularity of protection

MAPsec protection is specified per MAP operation. This gives reasonable protection granularity without introducing too much administrative overhead.

6.2 MAPsec protection groups

The following groups of messages and their protection modes are defined at both the operation level and the component level. Protection profiles can then be individual protection groups or particular combinations of groups.

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 on 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 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

6.2.1 MAP-PG examples

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 on situations where no security is required or is an option. This protection group cannot be combined with any other protection group.

Table 6: MAP-PG(1) – Protection for Reset

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
ResetContext-v2/ Reset	1	1
ResetContext-v1/ Reset	1	1

Table 7: MAP-PG(2) – Protection for Authentication Information except Handover Situations

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
InfoRetrievalContext-v3/ Send Authentication Info	2	3
InfoRetrievalContext-v2/ Send Authentication Info	2	3
InfoRetrievalContext-v1/ Send Parameters Not possible to make the protection dependant on the contents of the message	2	3
InterVlrInfoRetrievalContext-v3/ Send Identification	2	3
InterVlrInfoRetrievalContext-v2/ Send Identification	2	3

Table 8: MAP-PG(3) – Protection for Authentication Information in Handover Situations

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
handoverControlContext-v3/ Prepare Handover (Note that the AC contains also other operations)	2	4
handoverControlContext-v3/ Forward Access Signalling (Note that the AC contains also other operations)	2	T B D
handoverControlContext-v2/ Prepare Handover (Note that the AC contains also other operations)	2	4
handoverControlContext-v2/ Forward Access Signalling (Note that the AC contains also other operations)	2	T B D
handoverControlContext-v1/ Perform Handover (Note that the AC contains also other operations)	2	4
handoverControlContext-v1/ Forward Access Signalling (Note that the AC contains also other operations)	2	T B D

Table 9: MAP-PG(4) – Protection of Location Information

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
networkLocUpContext-v3/ Update Location (Note that the AC contains also other operations)	2	4
gprsLocationUpdateContext-v3/ Update GPRS Location (Note that the AC contains also other operations)	2	TBD (2 0 0)
handoverControlContext-v3/ Prepare Subsequent Handover (Note that the AC contains also other operations)	2	T B D (2 0 0)
subscriberInfoEnquiryContext-v3/ Provide Subscriber Info	2	3
networkLocUpContext-v2/ Update Location (Note that the AC contains also other operations)	2	4
handoverControlContext-v2/ Prepare Subsequent Handover (Note that the AC contains also other operations)	2	T B D (2 0 0)
networkLocUpContext-v1/ Update Location (Note that the AC contains also other operations)	2	4
handoverControlContext-v1/ Perform Subsequent Handover (Note that the AC contains also other operations)	2	T B D (2 0 0)

Table 10a: MAP-PG(5) – Protection of AnyTimeModification requests (a)

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
AnyTimInfoHandlingContext-v3 / AnyTimeModification	1	1

NOTE: This grouping cannot be combined with MAP-PG(6).

Table 10b: MAP-PG(6) – Protection of AnyTimeModification requests (b)

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
AnyTimInfoHandlingContext-v3 / AnyTimeModification	2	5

NOTE: This grouping cannot be combined with MAP-PG(5).

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 7 groups are defined, the rest are reserved for future use.

Table 11: 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	Location information
5	Anytime modification (a)
6	Anytime modification (b)
7-15	Reserved

The following examples of protection profiles can be defined.

Table 12: Standard Protection profiles examples

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)** ***Location information***	**PG(5)** ***Anytime modification (a)***	**PG(6)** ***Anytime modification (b)***
Profile A	✓						
Profile B		✓	✓				
Profile C		✓	✓	✓			
Profile D		✓	✓	✓	✓		
Profile E		✓	✓	✓	✓	✓	
Profile F		✓	✓	✓	✓		✓

Annex A (informative): Overview of Network Domain Security architecture for MAP application layer security

The material in this informative annex is intended for Release5 and will then be completed and made normative. The purpose of the annex is to capture the current SA3 working assumptions for Release5 of this TS. It has only been included in here to indicate the future direction of the Network Domain Security for MAP application layer security.

A.1 Network Domain Security Architecture for MAPsec

A.1.1 Key Administration Centres (KACs)

Key Administration Centres (KACs) are entities that are used for negotiating MAPsec SAs on behalf of MAP-NEs. The KACs are defined to handle communication over these interfaces:

- the Zd-interface, which is located between KACs from different MAP security domains. The IKE protocol with support for MAPsec DoI shall be used over this interface.
- the Ze-interface, which is located between a KAC and a MAP-NE within the same MAP security domain is used to transfer MAPsec SAs from KACs to MAP-NEs. The IKE and ESP protocols may be used to negotiate and secure the connection between the KAC and the MAP-NE.

When MAP-NEs need to establish a secure connection towards another MAP-NEs they will request a MAPsec SA from the KAC. The KAC will then either provide an existing MAPsec SAs or negotiate a new MAPsec SA, before returning the MAPsec SA to the MAP-NE.

A MAPsec SA is valid for all MAP communication between the two security domains for which it is negotiated. That is, the same MAPsec SA shall be provided to all MAP-NE in security domain A when communication with MAP-NEs in security domain B. Each security domain can have one or more KACs. Each KAC will be defined to MAPsec SAs towards a well-defined set of reachable MAP security domains. The number of KACs in a security domain will depend on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and to avoid single point of failures.

KACs perform the following operations:

- Negotiate SAs for MAPsec with other KACs belonging to other network operators. This action is triggered either by request for a MAP-SA by a NE or by policy enforcement when MAP-SAs always should be available. MAP-SAs negotiation is performed at Zd-interface using IKE protocol with MAPsec DoI.
- Perform refresh of MAP-SAs. Triggered internally by SA lifetime supervision, which is depending on the policies set by the operator and if, it is decided during the negotiation.
- Distribute MAP-SA information to requesting nodes belonging to the same Security Domain as the KAC. This is done according to the ‘RequestSA” procedure outlined in Annex A.3.
- (Optional) KAC may be able to establish IPSec connections supporting IKE with IPSec DOI in order to secure transmission of MAP-SAs to the NEs within its security domain.

KACs are also responsible for the maintenance of the following databases:

- KAC-SPDB-MAP: Defines the scope, the security policy, in which MAP-SAs may be negotiated (allowed MAP-PPs, Algorithms, SA-lifetimes, value of “Fallback to unprotected Mode Indicator”). This database is updated on operator initiative in the framework of the roaming agreements.
- KAC-SADB-MAP: Contains actual MAP-SA information as result of the IKE negotiation.

- (Optional) KAC-SPDB-IP: Defines the scope, the security policy, in which IPSec-SAs may be negotiated at the Ze-interface.
- (Optional) KAC-SADB-IP: Containing IPSec-SAs for protection of IP traffic between the KAC and NEs over the Ze-interface.

KACs are responsible for security sensitive operations and shall be physically secured. They shall offer capabilities for the secure storage of long-term keys used for IKE authentication.

A.1.2 UMTS key management and distribution architecture for SS7 and mixed SS7/IP-based protocols

The following section specifies the generic parts of the key management and distribution architecture for SS7 and mixed SS7/IP-based protocols. Due to the fact that the security mechanisms are found on the application layer a number of the issues are unique to the application.

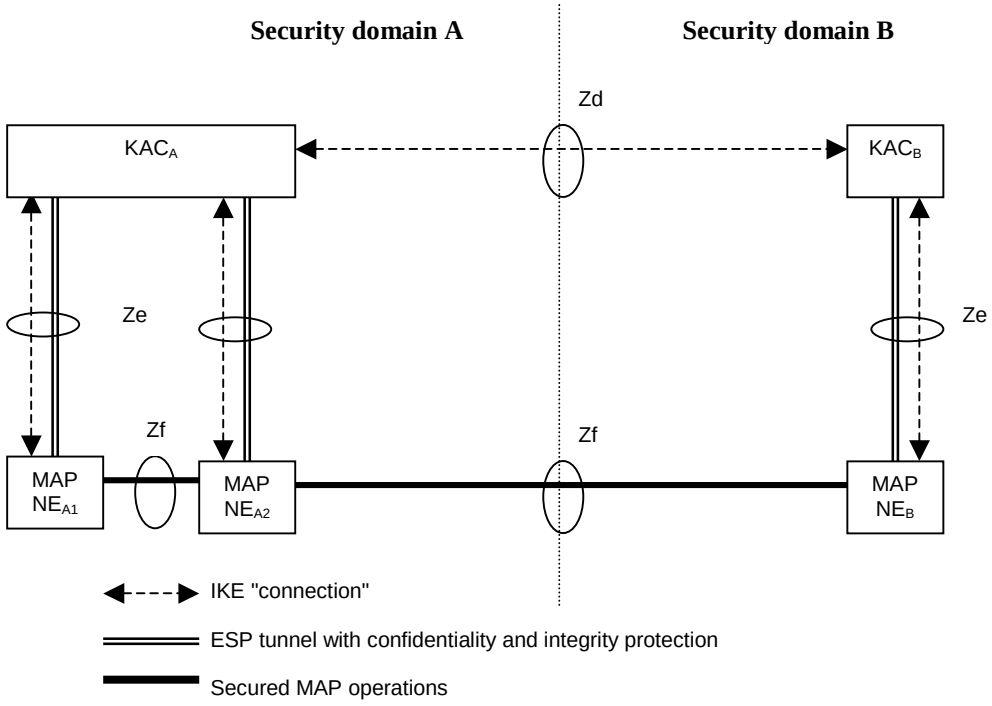

Figure A1: Overview of the Zd, Ze and Zf interfaces

The following interfaces are defined MAPsec.

- **Zd-interface (KAC-KAC)**

  The Zd-interface is used to negotiate MAPsec Security Associations (SAs) between MAP security domains. The traffic over Zd consists only of IKE negotiations. The negotiated MAPsec SAs are valid on a security domain to security domain basis.

- **Ze-interface (KAC-NE)**

  The Ze-interface is located between MAP-NEs and a KAC from the same MAP security domain. The KAC and the MAP-NE are able to establish and maintain an ESP tunnel between them. Whether the tunnel is established when needed or a priori is for the MAP security domain operator to decide. The tunnel is subsequently used for transport of MAPsec SAs from the KAC to the MAP-NE.

- **The Zf-interface (NE-NE)**

The Zf-interface is located between MAP-NEs. The MAP-NEs may be from the same security domain or from different security domains (as shown in figure A1). The MAP-NEs use MAPsec SAs received from a KAC to protect the MAP operations. The MAP operations within the MAP dialogue are protected selectively as specified in the applied MAPsec protection profile.

A.2 Inter-domain Security Association and Key Management Procedures

The overall architecture is defined in Annex A.1. This section only contains additional material to define the Zd-interface and the IKE protocol when used with the MAPsec DoI ([15]). Annex C contains material that complements the MAPsec DoI.

A.2.1 MAPsec required modifications to standard IKE

For MAPsec KAC←→KAC negotiation standard IKE Phase 1 shall be used. It is also required that only Main Mode shall be used for MAPsec.

A new Phase 2 mode - the MAP mode, must be introduced. The MAP mode differs from the existing IKE quick mode in the following respects:

- Payloads included to the messages of MAP mode are the same as in Quick Mode but the contents of the payloads differ in the case SA payload and ID payloads.
- Either the identity is never sent or if sent it will be the PLMDID in `fqdn` or `der_gn` encoded form (or the `key_id`).

KEYMAT for MAPsec SA template (as in the present Quick mode).

A.3 Local Security Association Distribution

A.3.1 General Overview

The following describes a network scenario with two MAP-NEs at different Security Domains (NEa and NEb) that whishes to communicate using MAPsec. Figure-A2 presents the proposed procedure for MAP-SA negotiation.

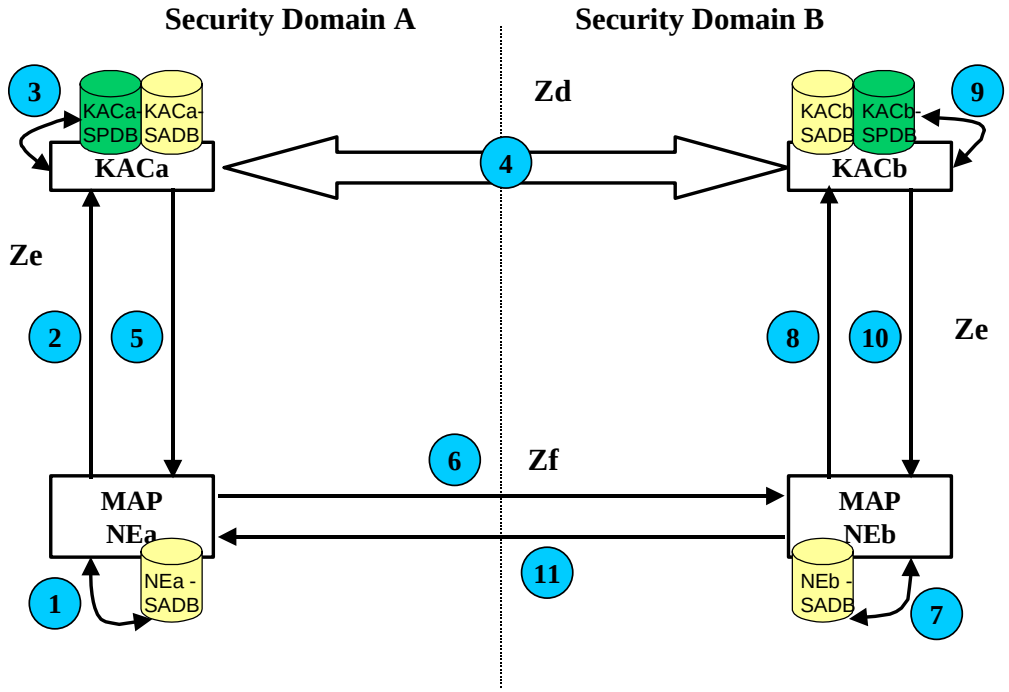

Figure-A2. MAP-SA Negotiation and Distribution Procedure

According to the Figure-A2, when MAP-NEa (NEa) from Security Domain A wishes to establish a secure communication with a MAP-NEb (NEb) of Security Domain B, the proposed process is the following:

1. NEa looks for a valid SA towards Security Domain B in its SADB. If it owns a valid SA, NEa starts the security protocol MAPsec (refer to step 6 below).

2. If NEa does not own a valid SA, then initiates a "RequestSA" procedure towards KACa, through Ze-interface.

3. KACa looks into its SPDB and SADB and checks the action:

   3.1. SPDB in KACa may indicate that communication towards Security Domain B does not need to be secured so KACa response to NEa MAP-SA request includes such indication (refer to step 5 below).

   3.2. SPDB in KACa may indicate that secure communication towards Security Domain B is required and KACa has a valid SA in its SADB for that purpose. KACa responds to NEa with the stored SA information (refer to step 5 below).

   3.3. SPDB in KACa may indicate that secure communication towards Security Domain B is required but KACa may not have a valid SA in its SADB for that purpose. KACa initiates a MAP-SA negotiation procedure with the KAC in Security Domain B, KACb (refer to step 4 below).

4. If KACa does not have a valid SA, KACa determines the appropriate KACb to negotiate SA according to SA end point, or domain identifier. KACa and KACb negotiate the SA through the Zd interface with IKE protocol using MAPsec DoI. KACb checks its SPDB to accept and complete the negotiation.

5. KACa responds to the "RequestSA" procedure initiated by NEa with a valid SA towards Security Domain B.

   This response to NEa might also indicate that secure communication towards Security Domain B is not required at that moment or that it has been impossible for KACa to provide a valid SA (e.g. problems during the SA negotiation with KACb, unavailability of KACb, etc …).

6. NEa stores information received and applies required actions:

   6.1. NEa generates MAPsec traffic towards NEb.

   6.2. NEa generated unprotected MAP traffic towards NEb.

   6.3. NEa aborts MAP communication towards NEb and any other NE within Security Domain B. NEa shall reattempt the "RequestSA" procedure when a new MAP communication is to be established towards Security Domain where NEb resides.

7. When NEb receives traffic from NEa, it checks its SADB for a valid SA to process traffic from Security Domain A. If NEb already has a valid SA, NEb can then continue security protocol MAPsec (refer to step 11 below).

8. If NEb does not own a valid SA, then initiates a "RequestSA" procedure towards KACb, through Ze-interface.

9. KACb looks for the already negotiated and stored SA information.

10. KACb responds to the "RequestSA" procedure initiated by NEb with a valid SA towards Security Domain A.

    This response to NEb might also indicate that secure communication towards Security Domain A is not required at that moment.

11. Finally, NEb can resume MAP communication towards NEa applying MAP Security depending on the content of the SA information received from KACb.

A.3.2 SA lifetime supervision at KAC and NEs

In order to improve processing time of the first message in a secure communication, the KACs and/or NEs might introduce the option to always maintain SAs alive.

With this option, KACs shall control the SA lifetime and negotiate a new SA before the SA in use expires in order to maintain continuously valid SAs for all or some pre-configured network domains. When a NE requests a SA, the KAC must answer with the recent one.

In a similar way and as a configuration option, NEs might supervise the SA lifetime and request a new one before the SA in use expires.

The following considerations must be noticed:

- All nodes might try to update their SAs at the same time, so in order to prevent KAC overload, SA requests from the NEs should be randomised.
- Two SAs can be valid during the same period of time; i.e. KAC might have negotiated a fresh SA before older one has expired.

A.3.3 Request SA Procedure

For local security association distribution a pure pull approached has been selected. The mechanism is outlined in more detail in Figure-A3.

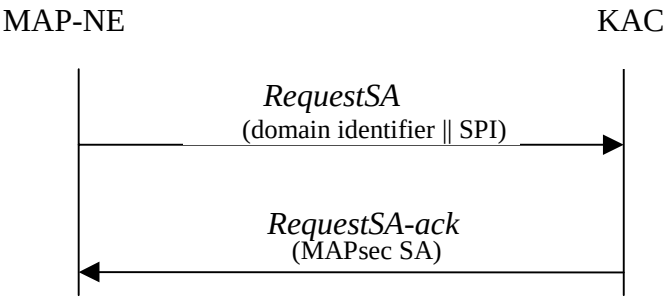

Figure A3: RequestSA procedure

The purpose of this procedure is to provide a MAP-NE with valid MAP-SA information to establish secure MAP communication with another MAP-NE.

The procedure is invoked by a MAP-NE when MAP communication towards another MAP-NE is to be initiated and no valid SA information is available at the MAP-NE SADB. Optionally, the procedure may also be initiated when the MAP-NE is configured to always maintain valid SAs.

The MAP-NE sends a *request SA* to the KAC; this message contains the domain identifier of the Security Domain the MAP-NE wishes to communicate with (i.e. destination PLMNid). In the event, the MAP-NE initiated the procedure with the purpose to refresh an existing SA (just expired or about to), the SPI (pair) of the SA being replaced shall be also included.

The answer from the KAC may include one of the following responses:

- Valid SA information to secure MAP communication to and from the Security Domain identified in the request.
- An indication that MAP communication towards/from that specific Security Domain does not need to be secured at that moment. This indication has a limited lifetime (also included in the response) to allow future changes in policy.
- An error response informing that the KAC is not able to provide the MAP-NE with valid SA information at that moment.

In order to perform this procedure in a secure manner, the KAC and MAP-NE might be able to use IKE to negotiate, establish and maintain an ESP tunnel between them. Whether the tunnel is established is for the MAP-Security domain operator to decide.

This procedure does not allow notification from KAC to MAP-NEs. If SAs are compromised, additional measures shall be applied in order to abort new or secure communication in progress (e.g. MAP Policy).

A.3.4 MAP-SA Information

KACs take information in their SPDBs to negotiate an SA pair (for inbound and outbound traffic respectively). Each component of the MAP-SA pair will be uniquely identified by the PLMNid and an SPI. The MAP-SA information downloaded to the MAP-NE in the course of an "RequestSA" procedure includes the following parameters for each component of the SA pair:

- **Encryption Algorithm Identifier:**

  Identifies the encryption Algorithm and its mode of operation used for confidentiality protection.

- **Encryption Key:**

  Encryption Key to be used for confidentiality protection.

- **MAC Algorithm Identifier:**

  Identifies the MAC Algorithm and its mode of operation used for integrity protection.

- **MAC Key:**

  MAC Key to be used for integrity protection.

- **MAP Protection Profile reference:**

  This field gives a reference to the chosen MAP protection profile. A MAP Protection Profile (MAP-PP), is a specification of how MAP operations over Zf-interface shall be protected. Indicates whether a MAP operation needs protection, and if so, indicates the protection mode to be used. The MAP-NE associates this reference to the actual MAP-PP.

- **Fallback to Unprotected Mode Indicator:**

  In case protection is required, this parameter indicates whether fallback to unprotected mode is allowed.

- **SA Lifetime:**

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

In the event, the KAC response includes the indication that MAP communication towards/from a specific Security Domain does not need to be secured at that moment, all the fields in the SA information will contain a NULL value except SA-lifetime. The value here will be treated as in the case of a normal MAP-SA (i.e. the MAP-NE will initiate a new "RequestSA" procedure when the SA-lifetime parameter indicates so).

In the event, the KAC response includes the error indication that the KAC is not able to provide the MAP-NE with valid SA information at that moment; the MAP-NE will abort the MAP communication towards the destination MAP-NE. The MAP-NE shall initiate a new "RequestSA" procedure next time a MAP message towards that security domain is required to be sent.

Annex B (informative): Guidelines for manual key management

[EDITOR:

The S3#17bis NDS ad-hoc meeting identified the need to provide some guidance for manual key management. I have assumed that an informative annex would suffice and I have also assumed that one would want to consider Zd and Ze separately. The material included here is **only** meant to trigger other contribution and is clearly insufficient by its own means.]

B.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)

B.2 Local Security Association Distribution (Ze-interface)

Manual Local Security Association Distribution is executed entirely within one security domain[1] 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 domain 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 **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

[1] Operators are expected define one security domain per network

Annex C (normative): Additional definitions for MAPsec DoI

The definitions contained in this annex are to be complementary to the definitions found in the MAPsec DoI RFC ([15]).

C.1 MAPsec SA definition

[EDITOR: We need to precisely define the MAPsec SA.]

C.2 Additional definitions for MAPsec DoI

[EDITOR: The S3#17bis NDS ad-hoc decided to split the MAPsec DoI into two parts. The main reason for this was to avoid having to update the MAPsec DoI RFC when the changes only really affected 3GPP MAPsec. So this annex is then to contain definitions that only applies to MAPsec and which S3 may change without having to update the RFC.

Needless to say: **CONTRIBUTIONS WANTED**]

Annex D (informative): Change history

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