3GPP TR 33.800 V0.4.0 (2001-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group SA3 3G Security; Principles for Network Domain Security; MAP application layer security (Release 5)

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 Report 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

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

The present document outlines the evolution of MAP security from the starting point defined by TS 33.200 v1.0.0 Rel4 and towards Rel5. The new functionality is mostly concerned with automated key management and distribution:

- Inter-domain Security Association and Key Management Procedures (Zd-interface)
- Local Security Association Distribution (Ze-interface)

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as 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-02.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 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:

C	MAP interface between an HLR and an MSC
D	MAP interface between an HLR and a VLR
E	MAP interface between MSCs
f6	MAP encryption algorithm
f7	MAP integrity algorithm
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	The MAP application layer security interface between MAP-NEs engaged in security protected signalling.

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

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 Network Domain Security Architecture for MAPsec

4.1 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.

4.2 UMTS key management and distribution architecture for MAP security

The following section specifies the generic parts of the key management and distribution architecture MAP security. Due to the fact that the security mechanisms are found on the application layer a number of the issues are unique to the application.

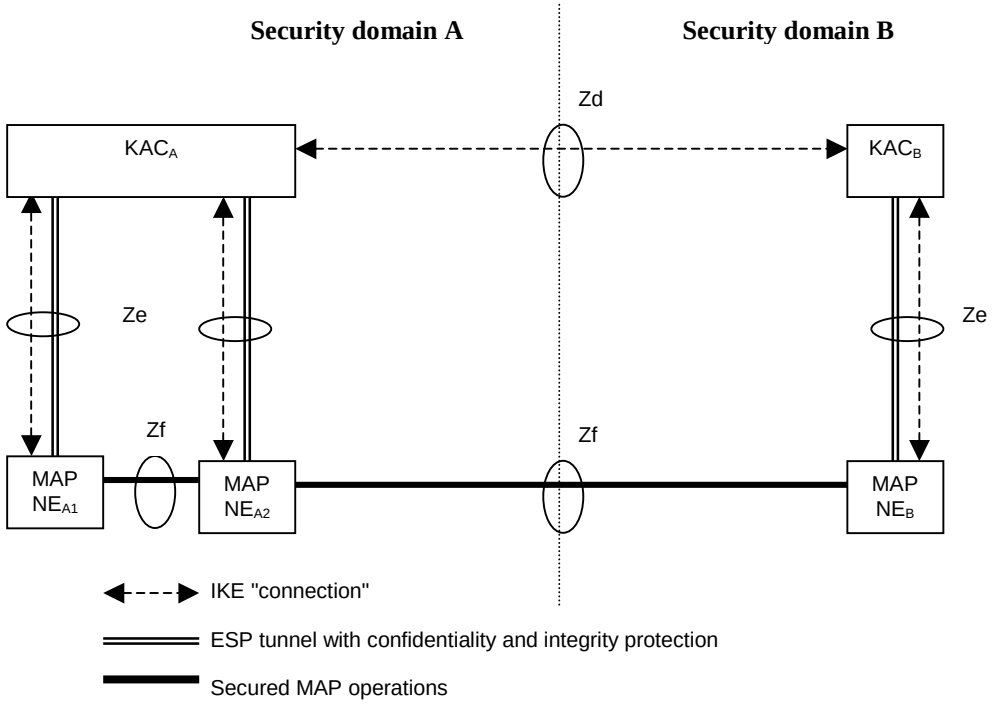

Figure 1: Overview of the Zd, Ze and Zf interfaces

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.

5 Inter-domain Security Association and Key Management Procedures

The overall architecture is defined in clause 5. This section only contains additional material to define the Zd-interface and the IKE protocol when used with the MAPsec DoI ([15]). Clause 7 contains material that complements the MAPsec DoI.

5.1 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).

6 Local Security Association Distribution

6.1 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-2 presents the proposed procedure for MAP-SA negotiation.

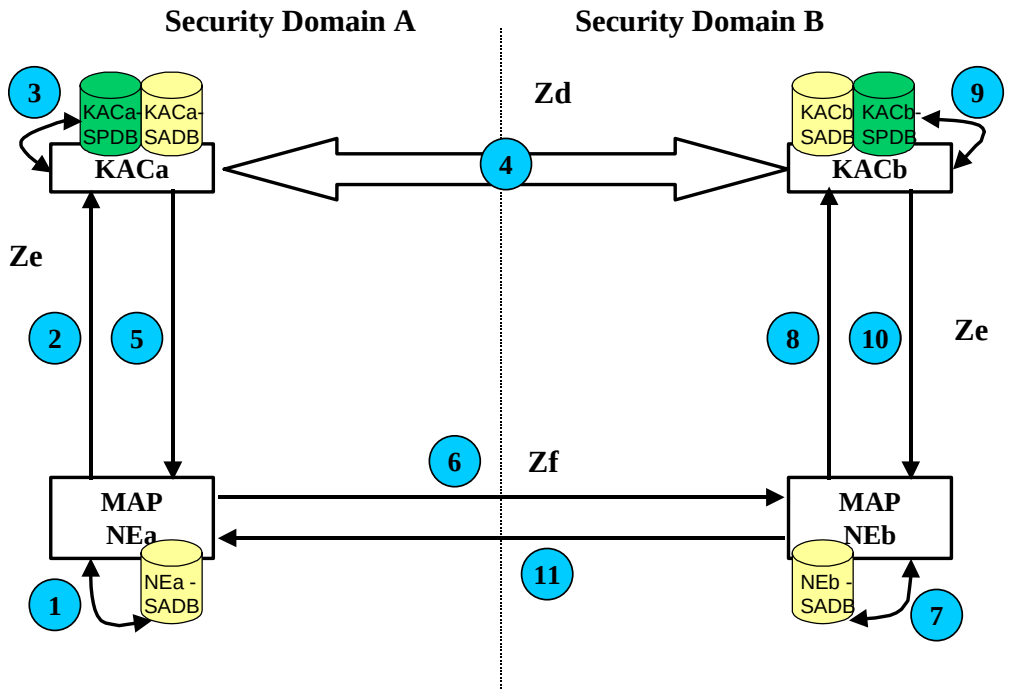

Figure-2. MAP-SA Negotiation and Distribution Procedure

According to the Figure-2, 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.

6.2 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.

6.3 Request SA Procedure

For local security association distribution a pure pull approached has been selected. The mechanism is outlined in more detail in Figure-3.

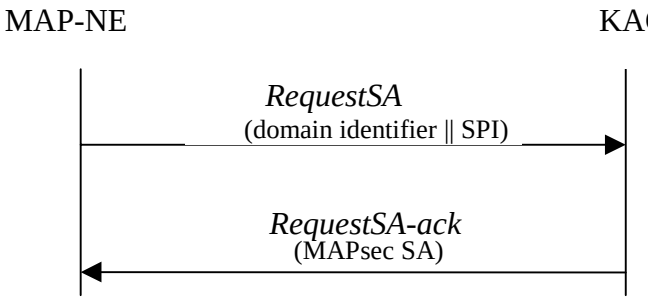

Figure 3: RequestSA procedure

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).

6.4 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.

7 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]).

7.1 MAPsec SA definition

7.2 Additional definitions for MAPsec DoI

Annex <A>: Change history

It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:

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