S3-000722

3G TS 33.200 V0.2.1 (2000-11)

Technical Specification

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

Keywords

Security, core network, 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 this network was the province of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions. Another significant development has been the introduction of IP in the GPRS backbone network. The introduction of IP signifies not only a shift towards packet switching, which is a major change by its own accounts, but also a shift towards completely open and easily accessible protocols. The implication is that from a security point of view, a whole new set of threats and risks must be faced.

For 3G systems it is a clear goal to be able to protect the core network 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 signalling in and between core networks. These include among the protocols MAP and GTP, among the interfaces Iu, and Iur, and possibly other protocols or interfaces that are new to R4 or have yet to be identified. The security characteristics that have been identified as being in need of protection are confidentiality, integrity, and authentication. These will be ensured by standard procedures, based on cryptographic techniques.

1 Scope

The present document defines the security architecture for the UMTS network domain. The scope of the UMTS network domain is to cover all of the UMTS core network with extension to cover the Iu-interface towards RNS. The design goals of the network domain security architecture are to cover the control plane and the associated signalling protocols.

The UMTS core network contains a number of SS7 based protocols, which in this specification is referred to as legacy protocols. While the stated goal of the network domain security is to cover all of the core network protocols, not all of the legacy protocols will be protected. 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 has been protected is the MAP protocol.

No security mechanisms are currently proposed for the CAP protocol.

Security protection for the Iu/Iur-interfaces will only be specified for the cases where the network layer is IP based.

It is explicitly noted that Lawful Interception consideration are covered in a separate specification.

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 TR 29.002: Mobile Application Part (MAP) specification

[4] 3G TR 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[5] 3G TS 33.102: Security Architecture

[6] 3G TS 33.103: Security Integration Guidelines

[7] 3G TS 33.106: <LI for R4, need version no>

[8] 3G TS 33.107: <LI for R4, need version no>

[9] 3G TS 33.120: Security Objectives and Principles

[10] 3G TS 33.800: Principles for Network Domain Security

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

[12] RFC-2402: IP Authentication Header

[13] RFC-2403: The Use of HMAC-MD5-96 within ESP and AH

[14] RFC-2404: The Use of HMAC-SHA-1-96 within ESP and AH

[15] RFC-2405: The ESP DES-CBC Cipher Algorithm With Explicit IV

[16] RFC-2406: IP Encapsulating Security Payload

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

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

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

[20] RFC-2410: The NULL Encryption Algorithm and Its Use With IPsec

[21] RFC-2411: IP Security Document Roadmap

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

[23] RFC-2451: The ESP CBC-Mode Cipher Algorithms

[24] IETF RFC-2521: ICMP Security Failures Messages

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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 uni-directional logical connection created for security purposes. All traffic traversing an SA is provided the same security protection. (this does not apply to IKE security association)

Transport mode: Mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers

Tunnel mode: Mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected

3.2 Symbols

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

Gc	Interface between a GGSN and an HLR.
Gd	Interface between a SMS-GMSC and an SGSN, and between a SMS-IWMSC and an SGSN.
Gf	Interface between an SGSN and an EIR.
Gi	Reference point between GPRS and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs.
Gr	Interface between an SGSN and an HLR.
Gs	Interface between an SGSN and an MSC/VLR.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
Iur	Interface between RNSs in the access network.
Za	Interface between KACs belonging to different networks, used for IKE
Zb	Interface between KACs and SEGs or KACs and NEs within the same network
Zc	Interface between networks for secure interoperation. Either SEG-SEG or NE-NE.

3.3 Abbreviations

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

AAA	Authentication Authorization Accounting
AH	Authentication Header
AKA	Authentication and key agreement
CS	Circuit Switched
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload
GGSN	Gateway GPRS Support Node
HLR	Home Location Register
IKE	Internet Key Exchange
ISAKMP	Internet Security Association Key Management Protocols
IV	Initialization Vector
KAC	Key Administration Centre
MAC	Message Authentication Code
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
RNS	Radio Network Subsystem
SA	Security Association
SAD	Security Association Database (sometimes also referred to as SADB)
SCTP	Stream Control Transmission Protocol
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SPD	Security Policy Database (sometime also referred to as SPDB)
SPI	Security Parameters Index
TVP	Time Variant Parameter
UE	User Equipment
UICC	UMTS IC Card
USIM	User Services Identity Module
USP	UMTS Security Profile
VLR	Visitor Location Register

4 Overall view of network domain security

4.1 Introduction

The scope of this section is to outline the basic principles for the network domain security architecture.

4.2 Security for SS7 and mixed SS7/IP based protocols

For legacy protocols, network entities must be able to provide security at the application layer. For legacy protocols over IP, network entities may optionally be able to provide security at the network layer, using IPsec.

If the transport for a legacy protocol is based on SS7 or on a combination of SS7 and IP, then security shall be provided at the application layer. If the transport for a legacy protocol is based on IP only, then security may be provided at the network layer exclusively or in addition to security at the application layer.

- MAP security shall be provided by the MAP security protocol. The MAP security protocol stage-3 specification is found in TS 29.002.

- MAP may optionally also be protected at the network layer when MAP/IP is available

- It is for further study whether other legacy protocols need to be considered.

4.3 Security for native IP based protocols

For native IP-based protocols, security shall be provided at the network layer. The security protocol to be used at the network layer is IPsec as specified in IETF RFC-2401 through RFC-2412. All network entities supporting native IP-based protocols shall support IPsec.

Note, that IPsec does not support the use of a single SA for hosts with multiple (a list of) IP addresses. Therefore care has to be taken while setting up GTP security where GSN nodes can have multiple IP addresses, or other protocols which offers support for multihomed hosts.

Key management for IPsec shall be automated.

4.4 Security domains

4.4.1 Security gateways

In order to support security for native IP-based protocols, a special type of network entities (NEs), called Security Gateway (SEG) entities, is defined. These entities shall offer the following functionality:

- SEGs operate at the border of a network, providing IP security for IP communication between different networks.
- SEGs shall be able to establish and maintain IPsec tunnels with any NE of their own network that use this SEG to secure IP traffic to different networks.
- SEGs must be able to establish and maintain IPsec tunnels with SEGs of other networks in order to secure IP traffic between networks. In particular, SEGs must be able to determine the IP address of an appropriate SEG of the destination network.
- SEGs must be able to let traffic, which need not be secured by the SEG, to bypass the security functionality.
- SEGs must interoperate with the network's firewalls to provide a maximum level of overall network security.
- An SEG must provide an interface to the entity providing the key management functionality

The key management functionality is logically separate from that of an SEG.

4.4.2 Security end points

In order to provide security for native IP-based protocols between network entities in the same network, an IPsec security association shall be established between these network entities.

In order to provide security for native IP-based protocols between network entities in different networks, there are two options:

- The endpoints of the IPsec security association coincide with the source and destination IP-addresses determined by the native IP-based protocol ("end-to-end IP security");
- The IP packets are routed via two Security Gateways, one in the originating network and one in the terminating network which terminate the IPsec security associations ("hop-by-hop IP security")

For secure IP traffic between network entities in different networks, **hop-by-hop IP security** shall be supported. This requires the originating NE to establish an IPsec tunnel to an appropriate SEG in the same network. The SEG terminates this tunnel and sends the data through another IPsec tunnel between the originating and the receiving network. This second tunnel is terminated by a second SEG, which in turn uses IPsec to pass the data to its final destination (path *a* in figure 1).

End-to-end IP security may be supported. This implies that an IPsec security association is established end-to-end between these NEs (path *b* in figure 1).

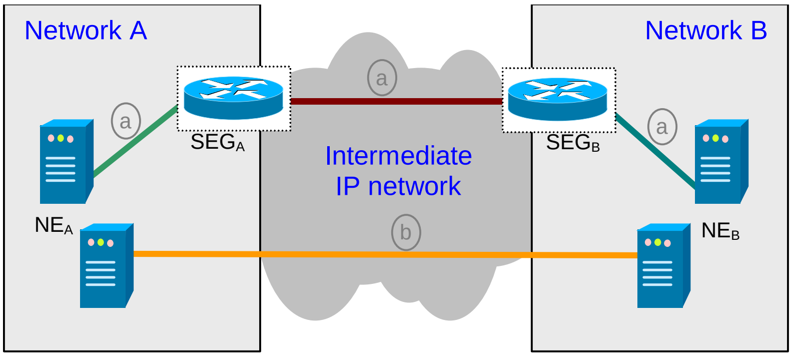

Figure 1: Options for secure IP communication between different networks

4.4.3 Security interfaces

ffs

4.4.4 The role of filtering routers and firewalls

ffs

5 Key management and distribution for UMTS networks

5.1 Security Associations (SA)

ffs

5.1.1 Security association functionality

ffs

5.1.2 Security Policy Database (SPD)

ffs

5.1.3 Security Association Database (SAD)

ffs

5.1.4 Security association bundles

ffs

5.2 UMTS key management and distribution architecture

5.2.1 The UMTS two-tiered key management and distribution architecture

The two-tiered key management architecture consists of two types of functional entities: key administration centres (KACs) and network entities (NEs). Security Gateways are considered a special kind of NEs. Each network includes at least one KAC[1]. Communication for two-tiered key management uses two interfaces, Z_A and Z_B, where Z_A connects different KACs and Z_B connects KACs with network entities (NE). Z_C is an interface between two network entities (NEs) which is to be secured.

- KACs communicate over Z_A to establish security associations (SA) for security protocols used over Z_C between two NEs in different networks. If the two NEs reside in the same network then one KAC may establish the required SAs, and communication between two different KACs over Z_A is not needed.
- Over Z_B these SAs are securely distributed from a KAC to NEs within the same network. Both push and pull mechanisms may be used.
- The security protocols used over Z_C protect legacy or native IP-based application layer protocols. These security protocols are specified in [doc/section, tba]. They include MAP/CAP security and IPsec.
- Security policy information is exchanged between KAC and NEs over Z_B. This information is required in the KAC and in the NEs, respectively, and depends on the security protocol used over Z_C. The definition of the security policy format for each security protocol can be found in [doc/section, tba].
- To secure SA negotiation and distribution, the two-tiered key management over Z_A and Z_B uses the IETF IPsec framework, cf. [IETF rfc2401, “Security architecture“].
- The KAC and all participating NEs must have an IP interface and support IPSec (AH and ESP) over the interfaces Z_A and Z_B. IPsec (AH and ESP) use the SA format described in IETF RFC 2407 when used over any of the interfaces Z_A, Z_B, or Z_C.
- A specification of the SA format for application layer security protocols over Z_C, such as MAP security

<u>Z_A interface:</u>

SAs for Z_C shall be established with IKE/IPsec between the KACs of different networks. The exact mechanism for SA establishment is described in [doc/section, tba]. According to the SA type required by the NEs for communication over Z_C, the KACs use the respective SA format for SA negotiation.

The implementation of IKE shall conform to IETF RFC 2409. In particular, for IKE Phase 1, authentication via pre-shared secrets shall be supported; support for other authentication methods is optional.

The KACs must be able to provide two classes of SAs to support inter- and intranetwork security over Z_C for NE and SEG entities:

- Class 1 SAs are NE-NE, SEG to NE or NE-SEG where both entities reside within the same network.
- Class 2 SAs are SEG-SEG where the SEGs reside in two different networks.

In addition, the KAC may be able to provide a third class of SAs to support inter-network security over Z_C for NEs:

- Class 3 SAs are NE-NE where the NEs reside in two different networks.

Note, that IPsec AH and ESP require an individual SA pair for each NE pair protected over Z_C. It is not possible to secure communication between more than one pair of NEs with a single SA pair. Furthermore, it is not possible to secure communication between NE pairs where NEs have more than one IP address (multi-homing), with a single SA pair.

[1] It is ffs whether it may be useful to have more than one KAC in a network.

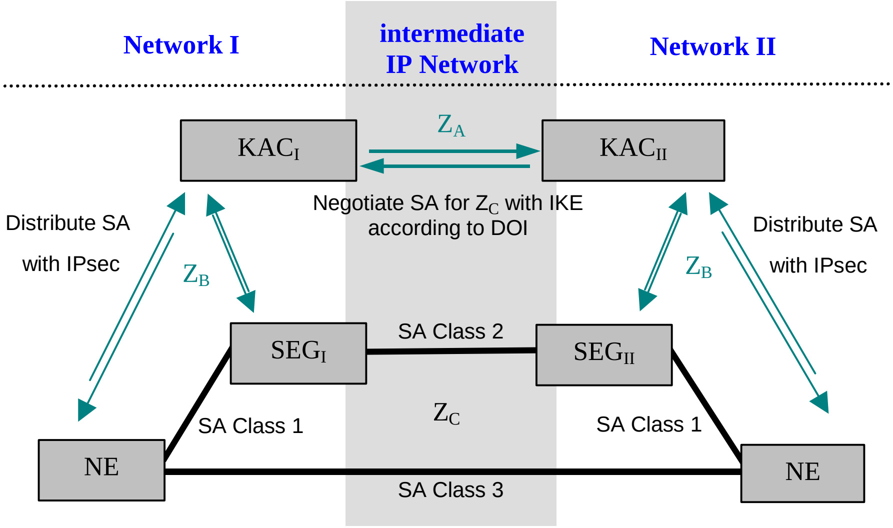

Figure 2: Two-tiered core network key management architecture

Z_B interface:

On the Z_B interface, IPsec shall be used to provide a secure channel between a KAC and an NE (or SEG) for distribution of the SAs used to secure Z_C and for exchanging the related policy information. If an automated key management with support for replay protection in IPsec is needed, IKE should be used. The implementation of IKE for the Z_B interface shall conform to IETF RFC 2409. If IKE is used for automated key management then, for IKE Phase 1, authentication via pre-shared secrets must be supported. Support for other authentication methods is optional.

The KAC mechanism to establish SAs for security protocols over Z_C is still regarded as an open issue:

- The first possibility to support IPsec replay protection for Z_C (which then requires automated keying) would be to negotiate the SAs between KACs with IKE as phase 2 SAs and pass them over Z_B to the NEs. To run IKE and the IPsec kernel (AH, ESP) on different logical entities is not the intention of the IPsec framework. It would necessitate to provide appropriate interfaces between the IKE entity, the IPsec kernel and the policy management component. Although this approach seems to be possible, it first has to be studied more careful whether it is in conflict with the IPsec RFCs and whether the implementation of such a system is possible.

- The second possibility is to establish a secure channel between the KACs and negotiate the SAs for ZC over this secure channel. This would require the specification of a new proprietary protocol for SA negotiation.

We prefer the first approach, under the reservation that the feasability of this approach can be shown and it does not offend the IPsec RFCs.

Z_c interface:

ffs

5.2.2 The use of Push vs Pull

ffs

5.3 Key management and distribution for native IP based protocols

5.3.1 Use of the Internet Key Exchange protocol

ffs

5.4 Key management and distribution for MAPsec

5.4.1 Use of the Internet Key Exchange protocol …?

ffs

6 Security for SS7 and mixed SS7/IP based protocols

6.1 The basic principles

ffs

6.1.1 Distribution and use of security associations

ffs

6.1.2 Authentication, Confidentiality, Integrity and Replay protection

ffs

6.2 Security for MAP

ffs

7 Security for native IP based protocols

7.1 The basic principles

ffs

7.2 Security services

7.2.1 Authentication, Confidentiality, Integrity and Replay protection

ffs

7.3 Security for GTP

ffs

8 Security for the Iu-interface

ffs

Annex A (normative): Support of IPsec in UMTS

ffs

Annex B (normative): UMTS Security Profiles (USP)

B.1 The UMTS Security Profiles

ffs

B.1.1 UMTS Security Profile for MAP

ffs

B.1.2 UMTS Security Profile for GTP

ffs

Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
12-2000	SA#10						