3GPP TSG SA WG3 Security — S3#16 **S3-000650**

28-30 November, 2000

Sophia Antipolis, France

Update information TR 33.800 v024 → v035

Here is the updated version of TR 33.800 as agreed at the Munchen ad-hoc. I have **not** done much more than what was agreed, even though chapter 5, 6, 7 and 8 could do with some tidying-up.

The most important changes:

- Overall: A number of editors notes have been deleted.
- ch2.1: removed self reference, included RFC-2960 (but I'm not entirely convinced that should keep it). Included TS 29.002, TS 29.060 and TS 33.200. Removed TR 23.821.
- ch2.2: the table containing the S3 references was to be deleted. Since that was the only real content, I've deleted the whole section
- ch3.3: a few abbreviations added including: TVP, IV, SCTP
- ch4.1 & 4.2 removed. Some text added directly under chapter 4.
- ch5.1.1: A-interface and Gb-interface reintroduced in table-1. Qualification with regard to coverage of NDS and interfaces/protocols found in table-1 added. A sentence to describe responsibility for Ga-interface added.
- ch5.2.2.1, figure-1: This figure has been marked by the **Comment** feature in word. The actual comment is that the figure shall not be part of TS 33.200. Parts of 5.2.2.1 removed as suggested in S3z000023.
- ch5.2.3: Fourth bullet point removed as suggested in S3z000023.
- ch5.3: CAP bullet removed.. Slightly modified the two other bullet points since they were formulated somewhat misleading.
- ch6: Peter Howard's stuff from Washington renumbered to ch6.0.x. I have not edited it. ***** IMPORTANT: Note that there may be major changes to chapter 6 depending upon the outcome of the investigation prompted by Siemens S3z000021. This will also affect chapter 7 and the MAPsec DoI.**
- ch6.2.1: Inclusion of push/pull in "Over the Zb these SA…" bullet point
- ch6.3: Within editors comments: References to BEANO removed.

- ch9: Some text to the effect that protocols over Iu/Iur will only be protected when using IP at the network level. (a one line sentence explaining this is also included in the Scope)
  This was suggested by me at the ad-hoc and people seems fairly happy about it. The decision must be confirmed/rejected by the SA3#16 plenary so please read it carefully.

- ch7.1.1: Section 7.1.1 removed;

- ch7.1.2: Last sentence removed. The whole section maked with **Comment** to the effect that it shall not be part of TS 33.200.

- ch.7.2.1: S3z000016. Proposed changes included. Minor addition to "SA liftetime" bullet to make the lifetime expressed as an absolute time reference(agreed at the ad-hoc). *Since the choice of absolute time means that we are deliberately breaking with the the IPsec DoI, I urge people to read this section carefully*. I have also taken the liberty of proposing a format for absolute time to progress matters.

- ch7.4.2: S3z000013. Proposed changes included. I took the liberty of replacing "encrypted hash" with "message authentication code".

- ch7.4.3: S3z000015. Proposed changes included.

- ch8.2.1: Some text moved from section 8.3.1 (not agreed at ad-hoc).

- ch8.3.5: Removed actual port numbers for GTP-C and GTP-U with reference to TS 29.060 and for preR99 a reference to GSM 09.60 is included.

14.11.2000 - Geir M. Køien

3GPP TR 33.800 V0.3.5 (2000-11)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Principles for Network Domain Security;
(Release 4+5)

Keywords
Network Domain Security, Key Management,
Architecture

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

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 A, 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 describes the guiding principles for the UMTS network domain security architecture. Many of the principles outlined in this document will be implemented and made normative in TS 33.200 Network Domain Security.

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 and the Iur-interface internal to the radio access network. 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 not covered by this technical report.

2 References

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

2.1 Numbered references

[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: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[6] 3G TS 33.103: Security Integration Guidelines

[7] 3G TS 33.120: Security Objectives and Principles

[8] 3G TS 33.200: Network Domain Security

[9] GSM 09.60: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[10] IETF RFC-1715 Randomness Recommendations for Security

[11] IETF RFC-2393: IP Payload Compression Protocol (IPComp)

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

[13] IETF RFC-2402: IP Authentication Header

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

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

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

[17] IETF RFC-2406: IP Encapsulating Security Payload

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

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

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

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

[22] IETF RFC-2411: IP Security Document Roadmap

[23] IETF RFC-2412: The OAKLEY Key Determination Protocol

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

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

[26] IETF RFC-2960: Stream Control Transmission Protocol

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:

Ga	Charging data collection interface between a CDR transmitting unit (e.g., an SGSN or a GGSN) and a CDR receiving functionality (a CGF).
Gb	Interface between an SGSN and a BSS.
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 Authorisation 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 Security threats and requirements

To firmly establish the security requirements for the network domain, a comprehensive security evaluation including threat analysis and risk assessment is a prerequisite. Having identified the security requirements one can then proceed to develop the actual security mechanisms, which subsequently can be implemented.

A thorough risk analysis and threat assessment study has already been carried out for UMTS, and it has been found that this study [1] contains sufficient coverage of the involved threats and risks for the network domain. The requirements derived from the threats and risks also seem to fulfill the needs for the network domain.

5 Overview of the network domain

5.1 Coverage of Network Domain Security

5.1.1 Protocols and interfaces covered by the network domain

The network domain consists of a number of interfaces and associated protocols. The actual number of interfaces is steadily increasing and so of course is the number of protocols within the network domain.

Table 1: Overview of the interfaces and protocols in the network domain

Interface	Protocols etc
A	Interface between MSC and BSC. Protocols over A include: - MTP, SCCP, BSSAP (which includes DTAP and BSSMAP)
Ga	Charging data collection interface between a CDR transmitting unit (e.g., an SGSN or a GGSN) and a CDR receiving functionality (a CGF).
Gb	Interface between an SGSN and a BSS. Notice that user plane and associated control plane data is protected by encryption between SGSN and the MS. Security parameters are not transported over Gb. Protocols over Gb include: - For the user plane: Frame Relay, BSSGP, LLC, SNDCP and IP - For the control plane: Frame Relay, BSSGP, LLC, GMM/SM
Gc	Interface between a GGSN and an HLR. This interface is optional, and the GGSN can route the required signalling towards HLR via a SGSN. Protocols over Gc: - MAP/SS7 (In the future: MAP/IP ??)
Gd	Interface between a SMS-GMSC and an SGSN, and between a SMS-IWMSC and an SGSN. Protocols over Gd: - SMS-TL carried by MAP/SS7 - In the future: SMS-TL carried by MAP/IP ??
Gf	Interface between an SGSN and an EIR. Protocols over Gf: - MAP/SS7 (In the future: MAP/IP ??)
Gi	Reference point between GPRS and an external packet data network. Protocols over Gi: - User plane IP - AAA signalling (typically RADIUS)
Gn	Interface between two GSNs within the same PLMN. Protocols over Gn: - Lower layer IP - GTP-C / GTP-U
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. Protocols over Gn: - Lower layer IP - GTP-C / GTP-U
Gr	Interface between an SGSN and an HLR. Protocols over Gc: - MAP/SS7 (In the future: MAP/IP ??)
Gs	Interface between an SGSN and an MSC/VLR Protocols over Gc: - MAP/SS7 (In the future: MAP/IP ??)
Iu	Interface between the RNS and the core network. It is also considered as a reference point. Protocols over Iu: - User plane PS: ATM, AAL5, UDP/IP, GTP-U - Control plane PS: ATM, AAL5, SSCOP, SSCF-NNI, MTB3b, SCCP, RANAP, GMM/SM/SMS - Control plane PS (alternatively): ATM, AAL5, UDP/IP, SCTP, ITUN, SCCP, RANAP, GMM/SM/SMS - User plane CS: ATM, AAL2, … - Control plane CS: ATM, AAL5, SSCOP, SSCF-NNI, MTB3b, RANAP, GMM/SM/SMS
Iur	Interface between RNSs in the access network. Protocols over Iur: - Control plane: same as for Iu-PS upto SCCP. Above SCCP one will find RNSAP - User plane: ATM, AAL2, …

Note: Table 2 is included for information. The actual coverage of the network domain security does not include all interfaces or all protocols.

5.2 Guiding principles for Network Domain Security

5.2.1 Introduction

The scope of this section is to outline the basic principles on which a security architecture for network domain should be based.

With the introduction of IP based transport to most, if not all, interfaces of the 3GPP specified network reference model follows new vulnerabilities of the network as well as new potential threats directed towards the network from outside. Instead of building, and managing, their own "private" transport networks, operators have a possibility to rent the transport capacity required between any two nodes of the reference model from virtually any ISP. Similarly also inter-network communications should not be considered unlikely to exploit the already existing transport network commonly known as Internet.

The most obvious security issue with such a view is that virtually any network connection could, in some sense, be considered "publicly" accessible and thus possible to exploit not only with the purpose of eavesdropping and fraud, but also with the purpose to attack the very business or reputation of the operator by means of e.g. hi-jacking, halting or in other ways disturbing the packet flow over such a connection.

The following sections discuss a basic architecture designed to support protected inter-network communications considering a scenario like the one described above. The very same principles might be applied, though, also for connections between e.g. two geographically separated sites within the same network.

5.2.2 The Security Architecture

5.2.2.1 The inter-network security architecture

The Security Gateway (SEG) is defined as a security entity located at the network border with the task to enforce the security policies, defined by the operator, concerning the packet flows between the own network and other networks. It can also be used to apply protection to packets exchanged directly with an external host, server or terminal if this is allowed by the policies.

It is envisioned that sensitive application level data - be it authentication data sent between the user and a service domain, a banking transaction, or any other sensitive data – will, and should, be protected using application level security mechanisms, since the trust relation in action is between the user and the application provider.
This means that data belonging to the user plane, i.e. packet flows over the Gi interface, will not be protected by the SEG, while all data belonging to the control plane will be protected by the SEG according to the relevant policies.

It is recommended that the SEG is placed in a network, a so called Extranet, which is separated from the internal network by a Firewall, FW. Typically also other network elements, like e.g. DNS servers and different types of proxies, could be located in such an Extranet. It is therefore also recommended to protect the Extranet itself by placing a second, outer Firewall between the Extranet and an external, shared transport network.

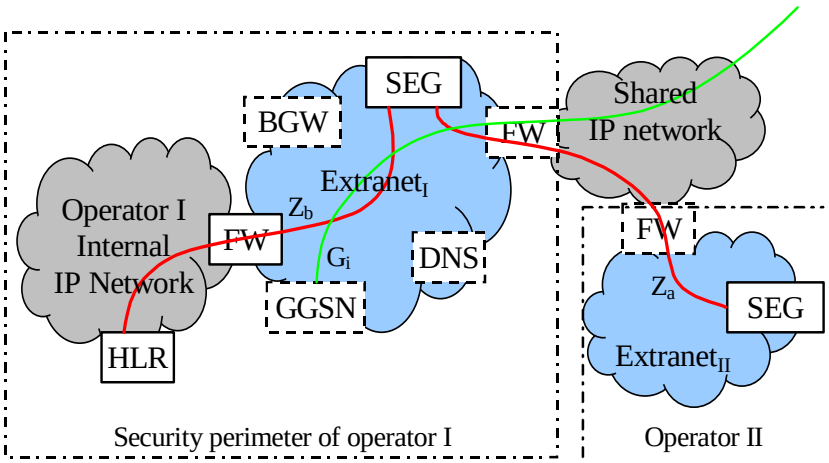

Fig. 1 An example security architecture

5.2.2.2 The intra-network security architecture

The choice of strategy for the protection of the internal network is an operator option. This means that no mechanisms, in this context, should be standardized as mandatory.

Considering that IPv6 seams likely to be chosen, not only to be used for UEs but also for network elements, and the fact that IPsec support is mandatory for all IPv6 implementations, it is reasonable to introduce IPsec as one optional way to secure a network internally. Support for IPsec for GTP in UMTS R4 and onwards is mandatory, but it is left as an operator option whether or not to use IPsec. This holds true for both IPv4 and IPv6 implementations.

IPsec may also be used to protect protocols other than GTP. The actual requirements will be specified in TS 33.200.

In such a scenario it is recommended to place an entity responsible for IPsec termination on the inside of the inner firewall. This would cause the inter-network traffic (still only the packets belonging to the control plane, as mentioned previously) to cross the firewall in clear, enabling that firewall to work in a stateful inspection mode or even as an Application Level Gateway (ALG) if so desired.

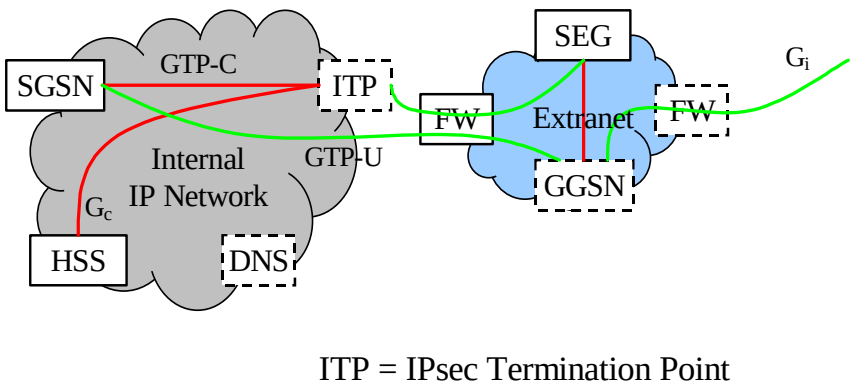

Fig. 2 An example on intra-network security (PS domain)

5.2.3 Recommendations

The security architecture outlined above, including the introduction of an Extranet together with the proposed new SEG entity, comes with several important benefits, such as:

- The security strategy regarding the intra-network connections remains clearly separated from the inter-network security strategy. This allows an operator to independently choose his/her own security strategy for the internal network, while still maintaining inter-operability with e.g. roaming partners by adopting the proposed architecture for the inter-network communications.
- Many "original" network elements/nodes can be leveraged from the processing burden and complex functionality imposed by many security functions and procedures, such as encryption, decryption, authentication etc.
- Due to the network-to-network approach of the architecture, as opposed to a generic node-to-node approach, the total number of required keys to manage decrease significantly, which allows for an operator to start off with a simple pre-shared keys strategy and wait with the deployment of PKI till a later stage.
- The proposed security architecture can be seen as a natural migration from the architecture presented in the key management solution for MAP as proposed by Ericsson (see T-Doc S3-000432), which ensures the ability to still employ node-to-node security in cases where this would be preferred.
- User plane traffic is NOT routed through a security gateway (SEG)
- User plane traffic (GTP-U) will not normally be protected by the operator network
- The actual configuration and deployment of the inner and outer firewalls as well as the extranet configuration is not to be standardised

5.3 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 run of 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 run of 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-2 specification is found in TS 33.200 and stage-3 specification is found in TS 29.002.
- MAP may optionally also be protected at the network layer
- It is for further study whether other legacy protocols need to be considered.

5.4 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, rfc2402(AH), rfc2406(ESP)]. All network entities supporting native IP-based protocols must 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 SCTP which offers support for multihomed hosts.

Key management for IPsec shall be automated to support IPsec replay protection.

5.5 Security domains

5.5.1 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.

5.5.2 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).

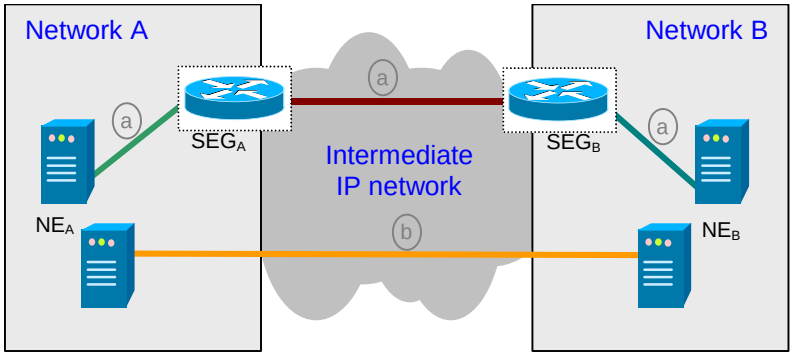

Figure 1: Options for secure IP communication between different networks

5.5.3 Security interfaces

[EDITOR: This section should specify the security interfaces and describe how they are used. The material for this section is currently found scattered around. (6.2.1 mostly)]

5.5.4 The role of filtering routers and firewalls

[EDITOR: Here we should detail the functional requirements that we have with respect to router filtering policies and firewall functionality. Some material found in description of extranet/intranet]

6 Key management and distribution for UMTS networks

6.0 Introduction

6.0.1 Working assumptions

1. A two-tiered key management architecture should be adopted in the first phase. Migration to a PKI-based flat key management will be considered for later phases.

2. IP-based communications secured using IPsec should be used for layer 1 and layer 2 which implies that all NEs and KACs support an IP stack.

3. IKE shall be used as the basis for key management (but some open issues need to be resolved - see below).

4. For communications secured using IPsec, the IETF IPsec security association will be adapted/profiled for 3GPP. For communications secured at the application layer, 3GPP will define new security associations (i.e. create a new DOI for ISAKMP). A first attempt at specifying a security association for MAPsec is given in S3-000433.

6.0.2 Open issues

1. Establishment of layer 3 SAs between KACs

There are two options: a) IKE is used; b) IKE is used between KACs to establish layer 1 SAs for IPsec between the KACs and another protocol is then used between the KACs to establish layer 3 SAs. Both options are described in S3-000445. The first option is favoured in S3-000432 (see start of section 4.3.1).

2. Establishment of layer 2 SAs between KACs and NEs

There are three options: a) IKE is used which implies that all NEs must support IKE; b) another protocol is used which implies a large specification effort; c) manual establishment which may be acceptable in the initial phase but which will require a proprietary anti-replay mechanism to be used. All options are described in S3-000445. The first option is favoured in S3-000432 (see end of section 4.3.4).

3. Distribution of layer 3 SAs to NEs

There are two options: a) a "push" approach using LDAP; b) a "pull" approach using SNMP. A preference for the first option is indicated in S3-000432. S3-000445 does not describe any options.

4. Achieving anti-replay protection at layer 3 for IPsec case

There are two options: a) a proprietary anti-replay mechanism is used; b) IKE based on the pre-shared secret established by layer 1/2 is used to dynamically negotiate SAs between NEs. Both options are described in S3-000445. S3-000432 does not describe any options.

6.0.3 Workplan

S3#15

- Resolve all the open issues listed above.

S3#16

- Write the stage 2 description of the IKE-based key management architecture.
- Select algorithms to be supported for MAPSec.
- Write MAPsec DOI for ISAKMP. Find out if it has to be an RFC.

- Agree on standard profiles of MAP-PP.
- Agree on use and format of SPI in the MAPSec component headers.
- Define database formats for SPD and SADB.
- Select algorithms to be supported for IPsec.
- Adapt IPsec DOI for ISAKMP. Find out if a new RFC is required.
- Select algorithms to be supported for CAP.
- Write CAPsec DOI for ISAKMP. Find out if it has to be an RFC.
- Agree on standard profiles of CAP-PP.

6.1 Security Associations (SA)

6.1.1 Security association functionality

6.1.2 Security Policy Database (SPD)

6.1.3 Security Association Database (SAD)

6.1.4 Security association bundles

6.2 UMTS key management and distribution architecture

6.2.1 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“].

---

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

- 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 (cf. [doc/section, tba]) can be found in [doc/section, tba].

Z_A interface:

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 preshared secrets must 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.

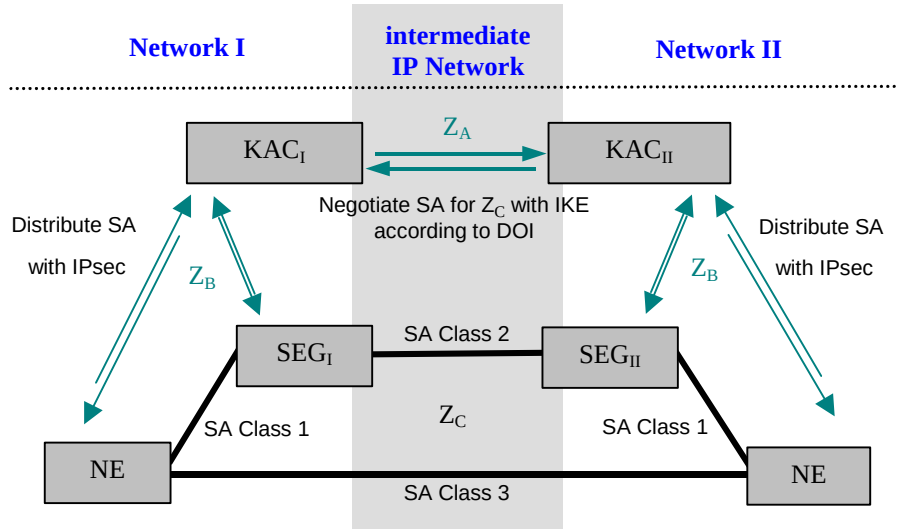

Figure 1: Two-tiered core network key management architecture

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 specification of the Z_B interface is described in [doc/section, tba].

NOTE: The proposed two-tiered model can be completely based on pre-shared symmetric keys for authentication or can use the public key authentication mechanisms of IKE. Using pre-shared symmetric keys means the KACs or NEs do not need to perform public key operations. Furthermore, no need for establishing a PKI (public key infrastructure) will arise for introducing core network security. But a smooth migration path from two-tiered to PKI-based security for later phases of UMTS development is possible.(cf. [doc/section, input from S3-000445, section3])

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.

6.2.2 The use of Push vs Pull

6.3 Use of the Internet Key Exchange protocol

[EDITOR: here we should spell out what we really need from IKE. For instance we may decide that we don't need perfect forward secrecy. We may also have ideas about requirements on the groups to be used by the Diffie-Hellman exchange. Furthermore, we may want to express preferences with respect to the algorithms that can be negotiated. We may want to exclude existing algorithms (say DES[2] and/or MD5).

*When it comes to authentication of the IKE SA (**not** the negotiated SA for use by ESP/AH) it can be done in five different ways.*

- using pre-shared secrets/keys

- using digital signatures based on DSS

- using digital signatures based on RSA

- using an encrypted nonce exchange (RSA based)

- using a revised encrypted nonce exchange (RSA based)

Siemens (S3-000560) have suggested to at least require support for the pre-shared secrets/keys option, which seems reasonable.]

6.4 Key management and distribution for MAPsec

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 new Domain of Interpretation (DoI) document must be produced. Such document should be published within the IETF framework as a separate RFC. Since the RFC would be concerned with non-IP issues it will most likely be an informational RFC, but it will nevertheless be normative for UMTS MAPsec purposes.

---

[2] In 2407 IESG have inserted a note to the effect that mandatory support of DES is about to be deprecated. Given the fact that an AES candidate now has been chosen I would assume that deprecation of mandatory DES support will occur when AES is formally adapted to IPsec. So to exclude DES is a real possibility.

6.4.1 MAPsec DoI for IKE/ISAKMP

RFC2408: ISAKMP 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

IANA will not normally assign a DoI value without referencing some public specification, such as an Internet RFC. Without a DoI value assigned by IANA, the MAP SA negotiation over the interface Z_A is not possible. MAPsec DoI for ISAKMP draft *must* be written, since the new DoI is an essential part of the key management architecture.

The following sections define briefly the requirements for MAPsec DoI for ISAKMP.

6.4.1.1 MAPsec Situation Definition

Within ISAKMP, the Situation provides information that the responder can use to determine how to process incoming SA request. For the MAPcec DoI, the Situation field is always left empty.

6.4.1.2 MAPsec Security Policy Requirements

The MAPsec DoI does not impose specific security policy requirements on any implementation.

MAPSec Assigned Numbers

The following sections list the Assigned Numbers for the MAPsec DoI: protocol identifiers and transform identifiers.

MAPsec Protocol Identifier defines a value for the Security Protocol Identifier referenced in an ISAKMP Proposal Payload for the MAPsec DoI.

Protocol ID	Value
PROTO_MAPSEC	5

It is recommended that the chosen value does not overlap existing IPsec DoI values.

MAPsec Transform Identifier defines at least one mandatory transform used to provide data confidentiality (The algorithms are just examples).

Transform ID	Value
RESERVED	0
MAPSEC_SHA1	1
MAPSEC_AES	2

It is recommended that operation mode (e.g. ECB, CBC) is combined to algorithms and not defined as a separate parameter. This will avoid configuration problems amongst other things.

6.4.1.3 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

6.4.1.4 MAPsec Payload Content

Defining different MAPsec payloads is outside the scope of this document. At least the following payloads require modifications or a redefinition:

- Security association payload
- Identification payload

6.4.1.5 MAPsec Key Exchange Requirements

MAPsec DoI does not introduce additional key exchange types.

6.4.2 Modifications to IKE

In Phase 1 there are no changes to main mode.

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)

6.4.3 Defining Policies and Structure of KAC-Z_A-SPD

The policy is described as in the RFC 2401 with following changes:

- The lifetime of the MAP SA is not defined as an amount of data transferred, but as 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* are no applicable.
- The operator defines for which networks MAP 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.

The SPD can be implemented as a text file to ease the porting to different systems. Text-file based implementation is also easier to alter by possible third parties than a GUI interface. The SPD file contains the information required to implement the security policy and does not require a lot of memory. It can be easily cached to improve the performance of the system (real time requirements).

6.4.4 Accessing KAC-Z_C-SADB

HTTP has been suggested as a protocol for fetching MAP SA's from KAC_Z_c_SADB. The KAC should then run a standard WEB server with a standard HTTP database.

7 Security for SS7 and mixed SS7/IP based protocols

7.1 The basic principles

7.1.1 Principles for securing for the MAP protocol

Although this section is discussing MAP, one should be aware that the same type of arguments applies to CAP.

It is assumed here that, for a long period after the introduction of IP as the transport for MAP, MAP/IP nodes (e.g. VLRs in network 1) need to be able to communicate with MAP/SS7 nodes (e.g. HLRs in network 2).

For MAP/IP security, there are basically two options:

- Security on the MAP application layer
- IP security (network layer security)

If IP security is used, the need for application-to-network layer security gateways (ANLSG) arise when interworking between IP and SS7 transport becomes necessary. Such an application-to-network layer gateway would have to translate application layer MAP security (in the SS7 domain) into network layer security (in the IP domain). This is highly undesirable for several reasons:

- There is high additional complexity introduced by such a gateway
- To receive protected MAP messages and to transform them into IPsec secured messages, a SS7/IP gateway must be capable of terminating application layer (MAP) security on the SS7 side. Since MAP routing is based on the IMSI number and does not happen at the MAP-layer, an SS7 end-entity cannot directly address (and usually does not even know) gateways at the network layer or other MAP entities. Therefore, it seems to be difficult to set up a MAP security association between a MAP end-entity and an ANLSG.
- The trust issues raised by this solution are difficult. The endpoints of the MAP communication would have to trust the ANLSG. But how can a MAP/SS7 node even know, which gateway the MAP messages pass? ANLSGs could even be located in intermediate networks, e.g. if the originating network has no direct link to the IP world. So ANLSGs were likely to influence and even restrict the worldwide PLMN topology, for guaranteeing a closed chain of trust between all communicating MAP entities.
- An ANLSG would seem to contradict the principle of a separation between transport stack and application.

This speaks in favour of providing security at the application layer also for MAP/IP.

On balance, this scenario isn't the only one. One may also require that all networks support both secure SS7 and IP based MAP version. This scenario does have some advantages like allowing for rapid transition toward IP-only networks, but it comes at the prohibitive cost of having two implementations for securing MAP.

A serious drawback of the application layer security approach is that every application protocols must be separately adapted to provide the desired security. In reality, this is not a serious problem as only MAP and CAP have been identified as targets for application layer security. Furthermore, the work to adapt MAP has already taken place.

Security for protocols that can be carried by both SS7 and IP should therefore be secured on the application layer. An additional advantage of this approach is that no additional specification and implementation effort is foreseen for MAP security when IP-based transport for MAP is introduced.

7.1.2 Overview of MAP security

The proposed mechanism consists of a two-tiered Key management architecture. For these purposes, a new NE at each network operator is introduced, the Key Administration Centre (KAC). Over the Z_A interface, KACs negotiate the Security Associations (SA), which then regulates the communication over the Z_C interfaces between the NEs of two different network operators. KACs also provide SA information to the relevant NEs via Z_B interface.

NEs then use the distributed SA information for the actual secure MAP signalling message transference at the Z_C interface.

Figure 20 provides an overview of the whole mechanism. Note that the protocols and message formats used at each interface are not specified in this figure. More details on the protocols and format of the messages at each interface will be provided in subsequent chapters.

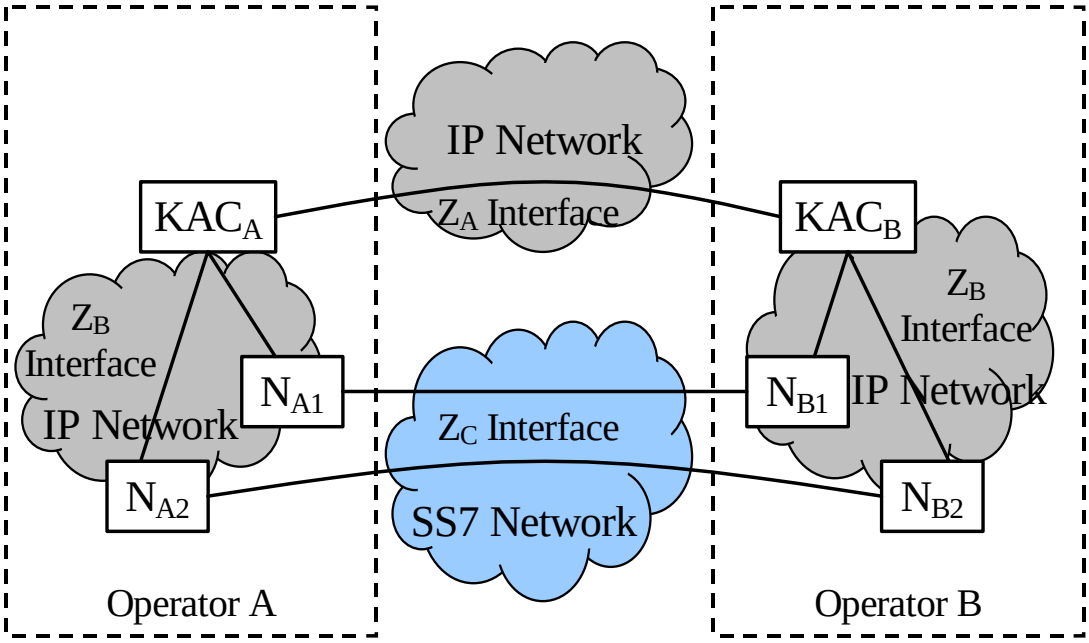

Figure 20: Overview of Proposed Mechanism

7.2 Distribution and use of security associations

7.2.1 Distribution of MAP-SA

A Security Association for Secure MAP message exchange (MAP-SA) is a set of policy and key(s) used to protect information. The MAP-SA conveys information about the security parameters to be used for MAP message protection when MAP messages are to be sent from Network A to Network B; i.e. a MAP-SA is a unidirectional SA (defined either for inbound or outbound traffic).

The agreement on a symmetric session key between two KACs for protection of the MAP message exchange between NEs belonging to their respective networks, is accomplished through the establishment of the MAP-SA.

A MAP-SA encompasses the following parameters:

- **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 an specification of how MAP operations over Z_C interface shall be protected. Indicates whether a MAP operation needs protection, and if so, indicates the protection mode to be used.

- **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.
  [EDITOR: Siemens suggested to only use absolute time at the ad-hoc and it was accepted. We should however not that this is in disagreement with RFC-2407 (DoI), which expresses SA duration in either Kbytes or seconds (Kbytes and seconds are the life type). The default duration in RFC-2407 is 28800 seconds (8 hours). Note that in RFC-2407 the duration **MUST** be specified in terms of the life types. Note also that RFC-2407 allows for lifetime to be specified in both Kbytes and seconds simultaneously.

  So if we choose to have absolute time we will, by design, have an incompatibility with the IPsec DoI.

  Provided that we still feel confident about using absolute time I take the liberty of proposing the following format:

	Year:	Month:	Day:	Hour:	Minute:	Second:	Time Zone
Digits: (Semi-octets)	2	2	2	2	2	2	2

  This format, of course, is the TP-Validity-Period for absolute time as found in TS 23.040 (v350) Short Message Service protocol. For more info see section 9.2 in TS 23.040 for coding details and 9.2.3.11 for explanation of the field itself.

  Of course, more compact representations are available, but ease of implementation is probably more important than saving a byte or two. Since this format is already in use in GSM/UMTS it should be easy to implement.

  ]

These parameters shall be transferred, in a secure manner, between the respective KACs of the co-operating networks at the Z_A interface.

The possibility to negotiate security attributes shall be provided to some extent, so that both communicating networks may arrange the encryption/MAC algorithms and parameters, the security policy or even the SA lifetime.

7.2.2 Properties and Tasks of Key Administration Centres

There is only one KAC per network operator. KACs perform the following tasks:

- Perform MAP-SA negotiation with 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.

- 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 valid MAP-SAs to requesting nodes belonging to the same network as the KAC. This is done according to the 'MAP-SA negotiation procedure' defined in subclause 7.2.3. The trigger for distribution can be implemented in different ways, see discussion on the Z_B interface below.

- (Option) Perform IKE negotiation and establish IPSec protection with NEs in its own network.

NOTE: The implementation of this option depends on whether the protocol selected for the Z_B interface provides security itself (AAA-based protocols) or requires additional security via IPSec (LDAP).

A KAC is also responsible for the maintenance of the following databases:

KAC-Z_A-SPD A database in the KAC, which defines the scope, the security policy, in which MAP-SAs may be negotiated.

KAC-Z_C-SADB A database in the KAC containing MAP-SAs and the corresponding MAP-PP entered and updated on operator initiative.

KAC-Z_B-SPD (Optional) A database which defines the scope, the security policy, in which IPSec-SAs may be negotiated at the interface Z_B.

KAC-Z_B-SADB (Optional) A database containing IPSec-SAs for protection of IP traffic between the KAC and NEs over the Z_B interface.

Due to these sensitive tasks, a KAC has to be physically secured.

7.2.3 Properties and Tasks of the Network Elements

NEs implementing secure MAP require the following additional functionality incorporated:

- Secure MAP according to MAP-SA for the network it communicates with.
- Maintain the NE-Z_C-SADB of valid MAP-SAs distributed from the KAC.
- Supervise MAP-SA lifetimes in the NE-Z_C-SADB.
- (Option) Perform IKE negotiation and establish IPSec protection with the KAC in its own network.

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

- NE-Z_C-SADB A database in a NE containing MAP-SAs and corresponding MAP-PPs.
- NE-Z_B-SADB (Optional) A database in a NE containing IPSec-SAs for protection of IP traffic between the NE and the KAC over the Z_B interface.

7.2.4 Key Management Architecture

7.2.4.1 Z_A Interface

Z_A Interface is an Inter-Networks interface between the KACs of two different network operators. Through this interface, the MAP-SA (or SAs) required to establish a secure communication between two NEs of each network are negotiated an agreed.

Z_A interface relies on IP transport and uses IKE with a MAP Domain of Interpretation (DOI) for ISAKMP to establish the MAP-SAs for MAP security.

NOTE: The MAP DOI needs to be developed and it should contain the parameters that can be negotiated. The goal here is to use the IPSec DOI as a starting point and preferably only change interpretation and range of values for the parameters negotiated in an IPSec IKE negotiation.

7.2.4.2 Z_b Interface

Z_B interface is an Intra-Network interface between the KAC and nodes capable of external communications using secure MAP. This interface is used for distribution of MAP-SAs and related information.

For example, an AuC will normally send sensitive authentication data (via the HLR) to VLRs/SGSNs belonging to other networks and will therefore get the MAP-SAs from its KAC.

Z_B interface is also assumed to rely on IP transport.

NOTE: The principles for MAP-SA distribution could be based on the KAC PUSHing MAP-SAs to all NEs or NEs PULLing the MAP-SAs from the KAC on demand. Adoption of PUSH based distribution guarantees that if a MAP-SA has been negotiated between two networks then it will be available in a NE when required. The KAC can also have central control of updating of SAs when they expire. It also has to handle failures to push a MAP-SA to a NE by regularly trying to resend the SA. The major drawback is that PUSHing SAs will introduce a lot of unnecessary traffic. With a PULL based system only needed MAP-SAs will be distributed. This minimises the traffic load. On the other hand the distribution must fulfil stricter time requirements.

In the case of adoption of the PUSH principle SNMP could be used to control and update the NEs databases (MIBs). If the PULL principle is adopted then LDAP can be used by the NEs to request information from the KAC. Another possibility in this case might be to place the SA info in a AAA server and use the appropriate protocol to fetch the information.

An initial evaluation at S3 favours a PULL based system using LDAP for SA distribution but this needs to be further discussed.

If the protocol selected for the Z_B interface does not provide security mechanism for a secure transfer of the MAP-SAs (LDAP), then IKE/IPSec should be employed.

7.2.5 MAP-SA negotiation procedure

When a NE_A in network operator A needs to communicate with a NE_B in network operator B, using Secure MAP, and it does not know of a valid MAP-SA to use for the receiving network, it contacts its KAC_A to get MAP-SAs (inbound and outbound) defined. The following steps define the procedures involved.

1. The NE_A requests a valid MAP-SA from the KAC_A
2. The KAC_A checks its associated MAP-SADB to see if there already is stored valid SAs for MAP connections to the network in question. If the KAC_A finds stored (valid) MAP-SAs, see step 7 below.
3. If the SADB does not contain valid MAP-SAs for the requested network, the KAC_A requests an IKE negotiation to establish them.
4. IKE checks if it has to perform phase 1 of the negotiation (if it has a valid ISAKMP-SA for the other KAC_B). If not see step 6.
5. The KAC_A contacts the KAC_B of the other network and starts phase 1 negotiations (main or aggressive mode depending on the policy set in the ISAKMP-SPD) of the required MAP-SAs (inbound and outbound traffic).
6. Then the KAC_A negotiates a new MAP-SAs by completing an 'IKE phase 2' procedure (quick mode) according to the policy it finds in its associated MAP-SPD.
7. The KAC_A forwards the MAP-SA to the requesting NE_A.
8. NE_A stores the received MAP-SAs and uses it for all communication towards the intended network until the MAP-SAs are no longer valid. (Then it all starts from 1 again.)

NOTE: This procedure follows the PULL approach.

7.2.6 Z_C Interface

Z_C interface is an Inter-Networks interface between two NEs of different network operators communicating by using secure MAP. This interface relies on MAP transport and policing and uses the distributed SAs information for securely exchanging sensitive data between the communicating NEs by means of a symmetric encryption algorithm. A block cipher shall be used for this purpose.

The secured (resp. authenticity/integrity-protected) messages are transported via the MAP protocol .

Z_C interface might be also implemented as an Intra-Network interface between two NEs of the same network operator. In this case, NEs receive the required MAP-SAs previously configured at the KAC (negotiation of MAP-SAs with a peer KAC over the Z_A interface is not required in this case.

7.3 Security services

7.3.1 Authentication, Confidentiality, Integrity and Replay protection

7.4 Security for MAP

This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN-VLRs/SGSNs and HE-HLRs belonging to different network operators and communicating with MAP protocols. Such procedures may be incorporated into the roaming agreement establishment process.

7.4.1 General Structure of Secured MAP Operations

Secured MAP operations are performed via the MAP protocol in the course of secured MAP dialogues.

For Secured MAP operations, three levels of protection (or protection modes) are defined providing the following security features:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, Authenticity

Secured MAP operations consists of a Security Header and the Protected Payload, that is the result of applying the corresponding protection mode to the original MAP operation payload. Secured MAP operations 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 operation . 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 operation in cleartext 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 operation.

Summing up, the Secured MAP Operation is a sequence of data elements consisting of the MAP Message Header, the Security Header and the protected payload. In the following subchapters, the contents of the protected payload for the different protection modes and the security header will be specified in greater detail.

7.4.2 Format of Secured MAP Message Body

7.4.2.1 Protection Mode 0

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

In case Protection Mode 0 is to be used, the mechanism shall also allow to perform the operation in cleartext, thus avoiding the extra load introduced by the Security Header.

7.4.2.2 Protection Mode 1

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

TVP||Cleartext|| $H_{KSXY(int)}$(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 session key KS_{XY}(int) 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 will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

7.4.2.3 Protection Mode 2

The Secured MAP Message Body in protection mode 2 takes the following form:

TVP|| $E_{KSXY(con)}$(Cleartext) || $H_{KSXY(int)}$(TVP|| MAP Header||Security Header|| $E_{KSXY(con)}$(Cleartext))

where "Cleartext" is the original MAP message in clear text. Message confidentiality is achieved by encrypting Cleartext with the confidentiality session key KS_{XY}(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and $E_{KSXY(con)}$(Cleartext).

The TVP used for replay protection of Secured MAP messages is a 32 bit time-stamp. The receiving network entity will 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 further recommended the use of protection mode 2 whenever possible as this makes replay attacks more difficult.

7.4.3 Structure of 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.

- **Initialization Vector (IV):**

  Initialization 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 issue is discussed in more detail in RFC 2406. IV has only local significance in the 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).

7.4.4 Mapping of MAP Messages and Modes of Protection

The network operator should be able to assign the mode of protection to each MAP message in order to adapt the level of protection according to its own security policy. Guidance may be obtained from the SS7 Signalling Protocols Threat Analysis [12].

It is foreseen that only a small set of MAP-PPs are standardised. However, the use of private MAP-PPs agreed offline between the operators shall be also allowed.

8 Security for native IP based protocols

8.1 The basic principles

8.2 Security services

8.2.1 Authentication, Confidentiality, Integrity and Replay protection

For control plane signalling messages, the provision of the following security services shall be provided:

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

All of the above security services can be provided by IPsec ESP mode.

8.3 Security for GTP

8.3.1 Using IPsec for protection of GTP

IPSec mainly consists of IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP). The Authentication Header provides data integrity, data origin authentication, and optional limited anti-replay services to IP. Encapsulating Security Payload provides confidentiality, data origin authentication, anti-replay, data integrity, and limited traffic flow confidentiality.

The concept of Security Association (SA) is fundamental to IPsec. The SAs are unidirectional contracts between two communication entities. SAs determine the IPsec protocols used for securing the packets, the algorithms, the keys, and the duration for which the keys are valid. A “Security Association Database” (SADB) maintains the SAs.

Both AH and ESP make use of SAs. A key management protocol IKE is employed to establish and maintain SAs. For UMTS purposes we assume that SAs are established by Key Administration Centres (KACs) defined in TS 33.102, so that both SADB and SPD are established for UMTS use. The security services afforded in the SAs will be applied to UMTS protocols as needed.

Use of ESP, AH, as well as any possible combination of them, should conform to standard IPsec to the extent possible.

Two types of SAs are defined in IPsec:

- **transport mode**
  In this mode only the higher layer protocols (transport and above) is protected by IPsec

- **tunnel mode**
  Tunnel mode provides for protection of the entire IP datagram, including the full original IP header information.

According to RFC 2401, “a host MUST support both transport and tunnel mode. A security gateway is required to support only tunnel mode. If it supports transport mode, that should be used only when the security gateway is acting as a host, e.g., for network management.”

For UMTS control plane messages, a host-to-host SA can be either transport mode or tunnel mode. However, whenever at least one end is a gateway, then it must be in tunnel mode. Furthermore, tunnel mode would provide source and destination address confidentiality. It must be noted that the use of tunnel mode is largely incompatible with the use of

NATs. This can be a problem in Ipv4 networks since address space is scare and NATs is common way of solving the address space problem.

GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 v3.5. It includes both the GTP control plane signalling (GTP-C) and user plane data transfer (GTP-U) procedures. GTP is defined for Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.

Some mobility management messages accommodated in GTP-C include sensitive information, for example, authentication vectors and MM context. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C). GTP-U is the tunnelling part of GTP, and as such GTP-U will itself carry user plane IP in its payload. Special care is required when applying security protection to GTP-U in order not to unnecessary duplicate protection on the two IP layers.

GTP uses UDP/IP path to transfer GTP signalling messages as well as to tunnel user data packets. IPsec is a set of protocols that integrate security into IP and provide data source authentication, data integrity, confidentiality, and protection against replay attacks. Therefore, IPsec is a natural candidate to provide protection for GTP messages.

8.3.2 Use of IPsec to protect GTP signalling messages

It is possible to protect both GTP signalling messages (GTP-C) and user data packets (GTP-U) by IPsec. However, in most of the applications, the user data may be protected by higher layer security mechanisms. It is not efficient or may not be necessary to apply double protection to user data.

Therefore it's generally assumed that the protection provided by IPsec only apply to GTP control plane signalling messages (GTP-C). Nevertheless, protection of GTP-U traffic by IPsec remains as an option for the network operators.

8.3.3 No changes to the GTP messages

IPSec is independent of any higher layer protocols. Therefore, it does not require any changes to the GTP messages. This differs from the approach taken to add security to MAP messages (in TS 29.002), where the security functions were applied at the application layer.

8.3.4 Error and failure handling

In RFC 2521, a set of ICMP messages are defined to deal with the errors and failures in using AH and ESP. The new ICMP messages defined include "bad SPI", "authentication failure", "decompression failure", "decryption failure", "need authentication", and "need authorization".

IPsec error status may be conveyed to the sender by means of a local network management function. This function is beyond the scope of GTP standardization.

8.3.5 IPsec SPD and its implication to GTP message protection

In the IPsec architecture, a look-up table, called Security Policy Database (SPD), is used to discriminate among traffic that is afforded IPSec protection and traffic that is allowed to bypass IPsec.

For any inbound or outbound datagram, three processing choices are possible:
- discard
- bypass,
- apply IPsec.

We recommend that GTP-U packets simply "bypass" the IPsec process and that GTP-C packets be afforded protection by the IPsec.

SPD specifies what security services are to be applied to an IP datagram based on a set of selectors, among which the most important ones are source IP address, destination IP address, source UDP port, and destination UDP port. The SPD must be consulted during the processing of all traffic (inbound and outbound), including non-IPsec traffic.

Different security mechanisms can be applied to GTP-C messages and GTP-U messages since they use different UDP ports (TS 29.060).

For Release99 and newer versions of GTP, this will allow us to apply IPsec mechanisms to only GTP-C messages. For pre-Release99 versions of GTP no port number distinction between GTP-C and GTP-U is made, and both GTP-C and GTP-U uses the same port number (GSM TS 09.60)

It may be possible to further classify GTP-C messages so that they can be protected by different security mechanisms, but it is a local matter for the application layer to signal the IPsec processing for selection of security mechanisms on a message-by-message basis.

8.3.6 IPsec protocols and applications to GTP messages

For GTP control plane signalling messages, the provision of the following security services is suggested:

- data integrity;
- data origin authentication;
- confidentiality; and
- anti-replay.

For GTP control plane messages, a host-to-host SA can be either transport mode or tunnel mode. However, whenever at least one end is a gateway, then it must be in tunnel mode. Furthermore, tunnel mode would provide source and destination address confidentiality.
Security services will probably also be needed to extend over the Gp interface, and thereby passing the Border Gateway (BG). This will imply mandatory support of tunnel mode.

9 Security for the Iu/Iur-interfaces

The Iu-interface between the SGSN/VLR and the RNC marks the boundary between the network domain proper and the radio access network. For practical reasons the Iu-interfaces has been included in the network domain. The Iur-interface between RNCs is an interface internal to the radio access network and it deals mostly with soft handovers. By definition the Iur-interface does not belong to the network domain, but it has nevertheless been included in the scope of network domain security.

The main motivation for including the Iu/Iur-interfaces in the network domain has been the need for protecting the keys CK and IK. These keys are transported from the SGSN/VLR to the RNC over the RANAP protocol and between RNCs over the RNSAP protocol. Both the RANAP and the RNSAP protocols can be carried by IP and/or SS7, depending on various options and whether the user is on CS or PS domain. For network domain security, the established principle is that protection of protocols carried by different network layers shall normally be done at the application layer. However, the complexity involved and amount of work required for protecting RANAP and RNSAP at the application level is prohibitively high compared to the relative benefits of gaining security protection for these protocols.

The approach taken for protection of Iu/Iur-interfaces therefore differs from the established principles for network domain security. There will be two general cases:

- The network/transport mechanism is SS7 based
- The network/transport mechanism is IP based

For the IP case, the protection shall be by means of IPsec in compliance with the IP based parts of network domain security architecture as detailed in the previous chapters. For the SS7 case no standardised protection scheme will be developed and it will be left to the vendors and operator how to protect the keys CK and IK over Iu/Iur-interfaces.

Annex A (normative): Support of IPsec in UMTS

[EDITOR: This section should spell out what our IPsec requirements are. It should probably be silent on what we don't need.]

A.1 Heading levels in an annex

Heading levels within an annex are used as in the main document, but for Heading level selection, the "A.", "B.", etc. are ignored. e.g. **B.1.2** is formatted using ***Heading 2*** style.

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

[EDITOR: I have put the definition of the various UMTS Security Profiles into an annex. The security profiles will serve as a UMTS version of the DOI used in IPsec. Except of course, that our profiles ought to narrow down the options available]

B.1 The UMTS Security Profiles

For each native IP-based protocol, profiles for the use of IPSec are specified. These may differ for different interfaces or may be identical. A security profile is a selection of options for the use of IPSec in the UMTS core network. When defining security policies and security associations for the use of IPSec [cf. IETF, rfc2401], the options selected in the security profile shall be used, thus reducing the IPSec configurations which need to be supported by the UMTS core network. A security profile need not completely determine the choice of security policies and security associations.

A security profile selects options for the following items:

- Security features: no security or integrity or integrity and confidentiality
- Security endpoint: end-to-end or hop-by-hop or both
- Security protocol: AH or ESP
- Mode: tunnel or transport mode
- Security mechanisms: a set of cryptographic algorithms which must be supported
- Selectors: the selectors which shall be used for security associations
- Mechanism for replay protection
- Support for SA lifetime handling
- Combination of security associations (if applicable)
- Failure handling
- Others [ffs]

B.1.1 UMTS Security Profile for MAP

[EDITOR: Here will have one or more USP for MAP. Some material is already present in the MAP section. This section may become obsolete.]

B.1.2 UMTS Security Profile for GTP

[EDITOR: Here will have one or more USP for GTP. This section may become obsolete.]

Annex <X>:
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