TSG-SA WG3 (Security) meeting #15 S3-000556
Washinton D.C., 12th September – 14th September 2000

Agenda Item:

Source: Ericsson

Title: R00 MAP Application Layer Security

Document for: Discussion and decision

1 Introduction

This contribution and accompanying CR tries to incorporate MAP application Layer Security into R00 TS 33.102 (it is assumed that the first version of TS 33.102 for R00 will be v.4.0.0).

The information included in the CR is based on the information removed from the specification for R99 but it also includes relevant agreements at S3 reached during the latest S3 meetings:

- **Tdoc S3-000368:** TVP used for replay protection defined as 32 bit time-stamp.
- **Tdoc S3-000382:** confidentiality and integrity protection are made independent of each other by making the hash function used to provide integrity protection a keyed hash function (MAC function); for a justification of this change see doc **S3-000312** with the amendment described in **S3-000355**.
- **Tdoc S3-000432:** Agreement of general working assumptions for key management (two tiered key management architecture, IKE on Z_A interface, discussion on PUSH/PULL for Z_B interface, …).
- **Tdoc S3-000433:** Draft definition of MAP-SA.
- **Tdoc S3-000478:** IP-based Z_B interface.

This CRs is intended to serve as a basis for further contributions in order to complete the WI according to the agreed principles and resolution of open questions. Therefore, further enhancements on the content of this CR are still foreseen, especially on the following issues:

Selection of a protocol for the Z_B interface (PULL with LDAP, PUSH with SNMP, AAA-based protocol).

Definition of MAP-DOI.

Definition of standardised MAP-PPs.

Definition of the structure of the Secured MAP messages and the Security Header.

3GPP TSG-SA3
Washington, D.C.
12-14 September 2000

Tdoc 3GPP S3-000556cr

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	CR	XXX	Current Version:	4.0.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: SA #9 *list expected approval meeting # here ↑*	for approval	X	strategic		*(for SMG use only)*
	for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: Ericsson **Date:** 06-09-00

Subject: R00 MAP application layer security

Work item: CNSS: Protection of MAP Application Layer

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature	X		Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	
				Release 00	X

Reason for change: Introduction of MAP application layer security in R00 specifications.
Introduction of latest agreements at S3 regarding this WI:

- **Tdoc S3-000368:** TVP used for replay protection defined as 32 bit time-stamp.
- **Tdoc S3-000382:** confidentiality and integrity protection are made independent of each other by making the hash function used to provide integrity protection a keyed hash function (MAC function); for a justification of this change see doc **S3-000312** with the amendment described in **S3-000355**.
- **Tdoc S3-000432:** Agreement of general working assumptions on key management (two tiered key management architecture, IKE on Z_A interface, discussion on PUSH/PULL for Z_B interface, …).
- **Tdoc S3-000433:** Draft definition of MAP-SA.
- **Tdoc S3-000478:** IP-based Z_B interface.

Clauses affected: 2.1, 3.3, 7

Other specs affected:

Other 3G core specifications		→ List of CRs:	TS 33.103
Other GSM core specification		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments: Modifications in this CR shall be incorporated to the version of 33.102 specification base of R00 (i.e. 4.0.0)

help.doc

<---------- Double-click here for help and instructions on how to create a CR.

-

2.1 Normative references

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] UMTS 33.21, version 2.0.0: "Security requirements".

[4] UMTS 33.22, version 1.0.0: "Security features".

[5] UMTS 33.23, version 0.2.0: "Security architecture".

[6] Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[7] TTC Work Items for IMT-2000 – System Aspects.

[8] Annex 8 of "Requirements and Objectives for 3G Mobile Services and systems" – "Security Design Principles".

[9] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.

[10] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques.*

[11] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).

[12] ETSI SMG10 WPB: SS7 Signalling Protocols Threat Analysis , Input Document AP 99-28 to SMG10 Meeting#28, Stockholm, Sweden.

[13] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[13a] 3G TS 23.003: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification".

[13b] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[13c] 3G TS 29.002: " 3rd Generation Partnership Project;Technical Specification Group Core Network; Mobile Application Part (MAP) specification".

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KAC	Key Administration Center
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MAP	Mobile Application Part
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
NE	Network Element
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SA	Security Association
SQN	Sequence number
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

7 MAP Application Signalling Security

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.

7.1 Overview of Mechanism

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 Center (KAC). Over the Z_A interface, KACs negotiate the Security Associations (SA) which rules 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.

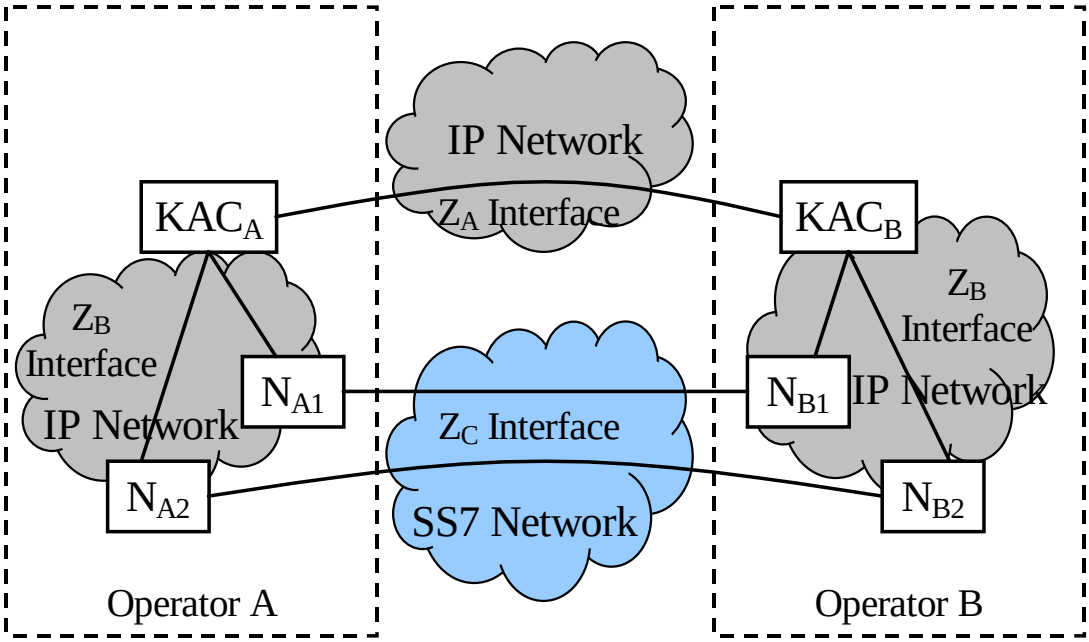

Figure 20: Overview of Proposed Mechanism

7.1.1 MAP Security Association

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 used for MAP message protection.
- **Encryption Key Version Number:**
  Version number of the encryption key to be used for MAP message protection.
- **Encryption Key:**
  Encryption Key to be used for MAP message protection.
- **MAC Algorithm Identifier:**
  Identifies the MAC Algorithm used for MAP message protection.
- **MAC Key Version Number:**
  Version number of the MAC key to be used for MAP message protection.
- **MAC Key:**
  MAC Key to be used for MAP message protection.
- **MAP Protection Profile:**
  A MAP Protection Profile (MAP-PP), is an specification of how components in a MAP message over Z_C interface shall be protected. Indicates whether a MAP dialogue needs protection, and if so, indicates for every component of the dialogue the protection mode and mode of operation of the encryption algorithm to be used. In case protection is required, it shall also state whether fallback to unprotected mode is allowed.
- **SA Lifetime:**
  Defines the actual duration of the SA.

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.

7.1.2 Properties and Tasks of Key Administration Centers

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.

7.1.3 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 Key Management Architecture

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.3 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 [13].

The secured (resp. authenticity/integrity-protected) messages are transported via the MAP protocol [13c].

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.

7.3.1 General Structure of Secured MAP Messages

Secured MAP messages are transported via the MAP protocol, that means, they form the payload of a MAP message after the original MAP message header. For Secured MAP Messages, 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 messages consists of a Security Header and the Secured MAP Message Body that is protected by the symmetric encryption algorithm, using the symmetric session keys that were distributed as part of the MAP-SA. Secured MAP Messages have the following structure:

Security Header	Secured MAP Message Body

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

Both parts of the Secured MAP message, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form in this proposal:

MAP Message Header	MAP Message Body

	Secured MAP Message

MAP Message Header	Security Header	Secured MAP Message Body

Like the security header, the MAP message header is transmitted in cleartext. In protection mode 2 providing confidentiality, the Secured MAP Message Body is essentially the encrypted "old" MAP message body. For integrity and authenticity, an encrypted hash calculated on the MAP message header, security header and the "old" MAP message body in cleartext is included in the Secured MAP Message Body in protection modes 1 and 2. In protection mode 0 no protection is offered, therefore the Secured MAP Message Body is identical to the "old" MAP message body in cleartext in this case.

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

7.3.2 Format of Secured MAP Message Body

7.3.2.1 Protection Mode 0

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

7.3.2.2 Protection Mode 1

The message body of Secured MAP messages in protection mode 1 takes the following form:

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

where "Cleartext" is the message body of the original MAP message in clear text. Therefore, in Protection Mode 1 the Secured MAP Message Body 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, MAP Header, Security Header and 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.

7.3.2.3 Protection Mode 2

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

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

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.

7.3.3 Structure of Security Header

NOTE: The content of the security header has yet to be finalised. Probably it will just contain the sending PLMN identity and an SPI identifying the MAP-SA used and per message related information like and Initialization Vector.

7.4 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.