3GPP TSG SA WG3 Security — S3#15bis **S3z000002**

3G TS 33.1de V0.0.1 (2000-10)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group SA3; Network Domain Security (Release 2000)

Keywords

Security, core network, key management

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This clause is optional. If it exists, it is always the third unnumbered clause.

1 Scope

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

The UMTS core network contains a number of SS7 based protocols, which in this specification is referred to as legacy protocols. While the stated goal of the network domain security is to cover all of the core network protocols, not all of the legacy protocols will be protected. Behind this is a realization that SS7 based legacy protocols can in practice only be protected at the application layer, and that the work involved in protecting the legacy protocols therefore will be high and require redesign of the protocol itself. Even in the cases were it would be technically feasible to do the job it is questionable whether the benefits would ever justify the required effort. Consequently, the only legacy protocol that has been protected is the MAP protocol.

2 References

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

[1] 3G TS 21.133: Security Threats and Requirements

[2] 3G TS 21.905: 3G Vocabulary

[3] 3G TS 33.102: Security Architecture

[4] 3G TS 33.103: Security Integration Guidelines

[5] 3G TS 33.120: Security Objectives and Principles

[6] 3G TS 33.9xx: Principles of Network Domain Security

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

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

[9] RFC-2402: IP Authentication Header

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

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

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

[13] RFC-2406: IP Encapsulating Security Payload

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

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

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

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

[18] RFC-2411: IP Security Document Roadmap

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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:

Symbol format

<symbol>	<Explanation>

3.3 Abbreviations

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

AH	Authentication Header
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
SA	Security Association
SAD	Security Association Database (sometimes also referred to as SADB)
SPD	Security Policy Database (sometime also referred to as SPDB)
SPI	Security Parameters Index
USP	UMTS Security Profile

4 Overall view of network domain security

4.1 Introduction

[This section is to describe that NDS is first and about security the UMTS CN control plane. So, while we don't exclude protection for the user plane we don't make too much of an effort to support it either.

There should also be a figure that illustrates the coverage of NDS. The figure should also include information about the security related interfaces.

To allow for security of the keys CK/IK the Iu-interface also needs to covered.

Furthermore this section should inform about differences between native-IP based protocols and mixed SS7/IP based protocols. This should end up in a description of the principle of using application layer security for mixed mode and IPsec for native IP. Then the section should go on to explain the "profiling" we have made of IPsec in general terms]

4.2 Security for SS7 and mixed SS7/IP based protocols

[This section will contain some justification of why application layer security has been chosen and how it generally should be applied. Furthermore it ought to make it clear that key mngt etc is done by IKE]

4.3 Security for native IP based protocols

[Similar to the above section except for that we will use network layer security for native IP protocols.

I'm presenting a case to (in a contribution that will be sent to the exploder late week-42):

- only use tunnel mode
- only use ESP
- make no use of PCP
- limit our use of SA-bundles

If this is accepted we should announce this here (without justification). We should also make it clear that these decisions are only mandatory with respect to roaming/interoperability and that operators may decide to deviate from this locally]

4.4 Security domains

[This section really defines the security architecture for NDS. It shall include detailed figures to illustrate the interfaces and their uses.]

4.4.1 Security gateways

[This section should detail the requirements and functionality of the SEGs. We should be careful as to what needs to be specified and what can be left to the vendors/operators]

4.4.2 Security interfaces

[This section should specify the security interfaces and describe how they are used.]

4.4.3 The role of filtering routers and firewalls

[Here we should detail the functional requirements that we have with respect to router filtering policies and firewall functionality. More general advice to be found in annex-c]

5 Key management and distribution for UMTS networks

5.1 Security Associations (SA)

[This section, with its subsections, shall introduce the concept of SAs. This includes the idea of SPD and SAD[1].]

[1] These are the correct abbreviations according to 2401. By the way, note that 2401 always uses the notation IPsec while most people seem to use IPSec. I shall follow the notation used by 2401.

5.1.1 Security association functionality

5.1.2 Security Policy Database (SPD)

5.1.3 Security Association Database (SAD)

5.1.4 Security association bundles

5.2 UMTS key management and distribution architecture

5.2.1 The UMTS two-tiered key management and distribution architecture

5.2.2 The use of Push vs Pull

5.3 Use of the Internet Key Exchange protocol

[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. For instance we may want to include UMTS specific algorithms (BEANO?) or 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 exhange (RSA based)

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

[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 Security for SS7 and mixed SS7/IP based protocols

6.1 The basic principles

6.1.1 Distribution and use of security associations

6.1.2 Authentication, Confidentiality, Integrity and Replay protection

[describe …

Require support for replay protection]

6.2 Security for MAP

[this sections should spell out exactly which security services that can be negotiated and which policies that may be had Furthermore we may want to be explicit about the algorithm choices that can be made. Details of the parameters etc to be found in the security profile for MAP in annex-b]

7 Security for native IP based protocols

7.1 The basic principles

[to describe the use of ESP in tunnel mode. …

Also show how SEGs are passed]

7.2 Security services

7.2.1 Authentication, Confidentiality, Integrity and Replay protection

[Here we should spell out how we use ESP/AH in tunnel/transport mode to achieve this or that security service]

We should also make it clear that we require support for replay protection, which can be supported be IPsec given that both parties actually uses it.]

7.3 Security for GTP

[this sections should spell out exactly which security services that can be negotiated and which policies that may be had (distinguishing GTP-U and GTP-C for instance). Furthermore we may want to be explicit about the algorithm choices that can be made. Details of the parameters etc to be found in the security profile for MAP in annex-b]

7.4 Security for <native IP protocol>

[just an illustrative placeholder – to be removed after the Munchen meeting]

8 Security for the Iu-interface

[ffs – though we need to agree if we shall consider this a part of our ambition . I feel we need it, although I can see that we may have to limit ourselves to the IP parts of the Iu-interface. Decision on ambition must be made at the November meeting.]

Annex A (normative): Support of IPsec in UMTS

[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)

[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

[Here will have to put some explanatory text to describe the idea of the security profiles]

B.1.1 UMTS Security Profile for MAP

[Here will have one or more USP for MAP]

B.1.2 UMTS Security Profile for GTP

[Here will have one or more USP for GTP]

Annex C (informative): Configuration issues for filtering routers and firewalls

[We should a have a short section discussing the use of filtering routers and firewall. Ideally, this section would then end up with a few references and general guidance. Its debatable whether it's a good idea to lay out concrete recommendations as the state of the art is a moving target.]

Annex <X> (informative):
Change history

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

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