International Telecommunication Union

ITU-T J.366.8

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(11/2006)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

IPCablecom2 IP Multimedia Subsystem (IMS): Network domain security specification

ITU-T Recommendation J.366.8

ITU-T Recommendation J.366.8

IPCablecom2 IP Multimedia Subsystem (IMS): Network domain security specification

Summary

This Recommendation introduces a new IPCablecom2 Recommendation to define the security architecture for the UMTS network domain IP-based control plane. The scope of the UMTS network domain control plane security is to cover the control signalling on selected interfaces between UMTS network elements.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

Source

ITU-T Recommendation J.366.8 was approved on 29 November 2006 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation J.366.8

IPCablecom2 IP Multimedia Subsystem (IMS): Network domain security specification

1 Scope

This Recommendation defines the security architecture for the UMTS network domain IP-based control plane. The scope of the UMTS network domain control plane security is to cover the control signalling on selected interfaces between UMTS network elements.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment. Additions are shown in blue underline and deletions in ~~red strikethrough~~.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

The modifications to ETSI TS 133.210 V6.5 (2005-01) Network Domain Security Specification are listed below.

2 References

<<Add the following references>>

[30] RFC 2246 "The TLS Protocol Version 1".

[31] RFC 3268 "AES Ciphersuites for TLS".

[32] RFC 3261 "SIP: Session Initiation Protocol".

[33] RFC 3546 "Transport Layer Security (TLS) Extensions".

[34] RFC 1750 "Randomness Recommendations for Security".

[35] RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

3 Definitions, symbols and abbreviations

3.1 Definitions

<<No Change>>.

3.2 Symbols

<<No Change>>.

3.3 Abbreviations

<<Add the following abbreviations>>

3DES Triple DES – a block cipher formed from the Data Encryption Standard (DES) cipher

CA Certification Authority

CBC Cipher Block Chaining

CRL Certificate Revocation List

DH Diffie-Hellman

EDE A 3DES mode where the data is encrypted, decrypted and encrypted

RSA An algorithm for public-key encryption invented by Ron Rivest, Adi Shamir and Len Adleman

SHA Secure Hash Algorithm

TLS Transport Layer Security

4 Overview over UMTS network domain security for IP-based protocols

4.1 Introduction

<<No Change>>.

4.2 Protection at the network layer

For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer are the IETF defined IPsec security protocols as specified in RFC 2401 [12]. Optionally, for the Zb interface, TLS may be used instead of or in addition to IPsec, as described in clause 6.

4.3 Security for native IP-based protocols

<<No Change>>.

4.4 Security domains

<<No Change>>.

4.5 Security Gateways (SEGs)

<<No Change>>.

5 Key management and distribution architecture for NDS/IP

5.1 Security services afforded to the protocols

<<No Change>>.

5.2 Security Associations (SAs)

<<No Change>>.

5.3 Profiling of IPsec

<<No Change>>.

5.4 Profiling of IKE

<<No Change>>.

5.5 Security policy granularity

<<No Change>>.

5.6 UMTS key management and distribution architecture for native IP-based protocols

5.6.1 Network domain security architecture outline

<<No Change>>.

5.6.2 Interface description

The following interfaces are defined for protection of native IP-based protocols:

– **Za-interface (SEG-SEG)**

  The Za-interface covers all NDS/IP traffic between security domains. On the Za-interface, authentication/integrity protection is mandatory and encryption is recommended. ESP shall be used for providing authentication/integrity protection and encryption. The SEGs use IKE to negotiate, establish and maintain a secure ESP tunnel between them. The tunnel is subsequently used for forwarding NDS/IP traffic between security domain A and security domain B. Inter-SEG tunnels can be available at all times, but they can also be established as needed.

  One SEG of security domain A can be dedicated to only serve a certain subset of security domains that security domain A needs to communicate with. This will limit the number of SAs and tunnels that need to be maintained.

  All security domains compliant with this specification shall operate the Za-interface.

– **Zb-interface (NE-SEG / NE-NE)**

  The Zb-interface is located between SEGs and NEs and between NEs within the same security domain. The Zb-interface is optional for implementation. If implemented, it shall implement ESP+IKE or TLS.

  On the Zb-interface, ESP shall always be used with authentication/integrity protection. The use of encryption is optional. The ESP Security Association shall be used for all control plane traffic that needs security protection.

  Whether the Security Association is established when needed or *a priori* is for the security domain operator to decide. The Security Association is subsequently used for exchange of NDS/IP traffic between the NEs.

NOTE 1 – The security policy established over the Za-interface may be subject to roaming agreements. This differs from the security policy enforced over the Zb-interface, which is unilaterally decided by the security domain operator.

NOTE 2 – There is normally no NE-NE interface for NEs belonging to separate security domains. This is because it is important to have a clear separation between the security domains. This is particularly relevant when different security policies are employed ~~whithin~~within the security domain and towards external destinations.

The restriction not to allow secure inter-domain NE-NE communication does not preclude a single physical entity to contain both NE and SEG functionality. It is observed that SEGs are responsible for enforcing security policies towards external destinations and that a combined NE/SEG would have the same responsibility towards external destinations. The exact SEG functionality required to allow for secure inter-domain NE←→NE communication will be subject to the actual security policies being employed. Thus, it will be possible to have secure direct inter-domain NE←→NE communication within the framework of NDS/IP if both NEs have implemented SEG functionality. If a NE and SEG is combined in one physical entity, the SEG functionality of the combined unit should not be used by other NEs towards external security domains.

6 TLS Option for Protection of Intra-Network SIP

The use of TLS is optional. TLS may be supported on the Zb interface (see Figure 1) for security of intra-network TCP interfaces.

The TLS protocol provides privacy and data integrity over a reliable transport layer protocol such as TCP. This means that UDP-based protocols will not be able to use TLS. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol is used to securely encapsulate upper layer protocols, while the TLS Handshake Protocol provides the key management functionality required to establish and manage TLS sessions.

If TLS is supported, the NE shall implement the requirements specified in this clause. Unless specified within this clause, interfaces requiring TLS shall be compliant with the TLS specification [30]. Additionally, SIP interface that requires TLS shall comply with any requirements specified in [32] relating to the usage of TLS in SIP.

TLS [30] supports the negotiation and use of compression methods. However, since these methods are not specified within TLS [30], compression shall not be used.

Note that TLS is the IETF standardized successor to the Secure Socket Layer (SSL) protocol. TLS has security enhancements over the SSL protocol. See [30], [31], and [33].

6.1 TLS Authentication Algorithms

The HMAC-SHA-1 (with 160-bit key) algorithm shall be supported in order to provide data origin authentication and data integrity services in TLS. AES-XCBC is not required.

6.2 Key Exchange Algorithms for TLS

Following are the requirements relating to methods for key exchange within the TLS protocol:

– RSA shall be supported;

– Diffie-Hellman (DH) shall be supported.

6.3 Random Number Generator for TLS

Random number generation implementations tend to be weak. Many semiconductor manufacturers are adding secure random number generators to their integrated circuits, which should be used if available. If no hardware is available, strong pseudo-random number generator software may optionally be used following the guidelines in [34].

Following are the requirements relating to random number generation:

– A hardware random number generator may be supported.

– Pseudo-random number generator software shall be supported if a hardware random number generator is not supported.

6.4 TLS Encryption Algorithms

Following are the TLS Client and TLS Server requirements related to encryption algorithms:

– 3DES CBC-mode (with 3 independent 56-bit keys) shall be supported.

– AES CBC (with 128-bit key) shall be supported.

– Null encryption may be supported.

6.5 Ciphersuites for TLS

TLS specifies various ciphersuites for use within the TLS protocol, as discussed in detail in [31]. Ciphersuites represent the recommended combinations of encryption, authentication, and key exchange algorithms to be used within the TLS protocol.

Following are the requirements related to Ciphersuites for TLS:

– "TLS_RSA_WITH_AES_128_CBC_SHA" shall be supported.

– "TLS_DH_RSA_WITH_AES_128_CBC_SHA" shall be supported.

– "TLS_RSA_WITH_3DES_EDE_CBC_SHA" should be supported.

– "TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA" should be supported.

– "TLS_RSA_WITH_NULL_SHA" may be supported.

6.6 TLS Authentication

TLS allows either unidirectional authentication where the server is authenticated to the client only, or bidirectional authentication where both client and server authenticate to each other. Unidirectional authentication is the usual method used in the public Internet; however, for network signalling and control applications, bidirectional authentication is mandatory to allow both parties to know they are communicating with the desired endpoint.

Following is the requirement related to TLS authentication:

– Bidirectional authentication for TLS applications shall be supported.

6.7 TLS Certificate Profile

X.509 digital certificates [35] are used for authentication in TLS. All X.509 certificates should be signed by a trusted party.

Table 1a/J.366.8 – TLS Certificate Profile

Server Certificates	
Subject Name Form	C=<Country> O=<Company> CN=<FQDN> Additional fields may be present in the subject name. FQDN is the server's fully qualified domain name (e.g., server.example.com). Only a single FQDN is allowed in the CN field.
Intended Usage	These certificates are used to authenticate TLS handshake exchanges (and encrypt when using RSA key exchange).
Validity Period	Set by operator policy
Modulus Length	1024, 1536, 2048
Extensions	KeyUsage[critical](digitalSignature, keyEncipherment) extendedKeyUsage[critical] (id-kp-serverAuth, id-kp-clientAuth) authorityKeyIdentifier[critical](keyIdentifier=<subjectKeyIdentifier value from CA cert>)

6.8 Certificate Validation

TLS certificates shall be verified as part of a certificate chain that chains up to a trusted Root certificate. The chain may contain intermediate Certification Authority (CA) certificates. Usually the first certificate in the chain is not explicitly included in the certificate chain that is sent over the wire. In the cases where the first certificate is explicitly included, it shall already be known to the verifying party ahead of time and shall not contain any changes to the certificate, with the possible exception of the certificate serial number, validity period and the value of the signature. If changes other than the certificate serial number, validity period and the value of the signature, exist in the root certificate that was passed over the wire in comparison to the known root certificate, the device making the comparison shall fail the certificate verification.

The NE shall build the certificate chain and validate the TLS certificate according to the "Certificate Path Validation" procedures described in [35]. In general, X.509 certificates support a liberal set of rules for determining if the issuer name of a certificate matches the subject name of another. The rules are such that two name fields may be declared to match even though a binary comparison of the two name fields does not indicate a match. RFC 3280 [35] recommends that certificate authorities restrict the encoding of name fields so that an implementation can declare a match or mismatch using simple binary comparison. Accordingly, the DER-encoded tbsCertificate.issuer field of a certificate shall be an exact match to the DER-encoded tbsCertificate.subject field of its issuer certificate. An implementation may compare an issuer name to a subject name by performing a binary comparison of the DER-encoded tbsCertificate.issuer and tbsCertificate.subject fields.

6.9 Certificate Revocation

Certificate Revocation Lists (CRLs) may be checked as part of certificate path validation. The CRL profile and how a NE obtains a CRL is not defined.

Annexes A-D

<<No Changes>>.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007