

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.7

(08/2010)

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

IPCablecom

**IPCablecom2 IP Multimedia Subsystem (IMS):
Access security for IP-based services**

Recommendation ITU-T J.366.7

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Recommendation ITU-T J.366.7

IP-Cablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services

Summary

Recommendation ITU-T J.366.7 specifies the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system as modified for use in cable networks.

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.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.366.7	2010-08-29	9

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	1
5	Conventions	1
6	Modifications to [ETSI TS 133.203]	2

Recommendation ITU-T J.366.7

IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services

1 Scope

This Recommendation specifies the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system as modified for use in cable networks.

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.

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.

Because this Recommendation indicates modifications from the ETSI specification [ETSI TS 133.203], the structure of the Recommendation does not follow normal ITU-T practice, so as to ease the task of the reader to correlate the two documents.

The modifications to the access security for IP-based services specification [ETSI TS 133.203] are shown in clause 6.

2 References

[ETSI TS 133.203] ETSI TS 133.203 V6.9.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the terms defined in [ETSI TS 133.203].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the abbreviations provided in [ETSI TS 133.203].

5 Conventions

This Recommendation uses the conventions provided in [ETSI TS 133.203].

6 Modifications to [ETSI TS 133.203]

Modifications introduced by this Recommendation are shown in revision marks. Unchanged text is replaced by ellipsis (...). Some parts of unchanged text (section numbers, etc.) may be kept to indicate the correct insertion points.

...

2 References

...

- [25] 3GPP TR 33.978: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Aspects Of Early IMS".
- [26] IETF RFC 5626 (2009), *Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)*.
- [27] OMA WAP-211-WAPCert, 22.5.2001,
<http://www.openmobilealliance.org/tech/affiliates/wap/wap-211-wapcert-20010522-a.pdf>.
- [28] IETF RFC 1750 (1994), *Randomness Recommendations for Security*.
- [29] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.
- [30] OMA WAP-219-TLS, 4.11.2001, <http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf>.
- [31] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

...

3.3 Abbreviations

...

SIP Session Initiation Protocol

TLS Transport Layer Security

4 Overview of the security architecture

...

The mechanisms specified in this technical specification are independent of the mechanisms defined for the CS- and PS-domain.

An independent IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IMS would continue to be protected by its own security mechanism. As indicated in figure 1 the P-CSCF may be located either in the Visited or the Home Network. The P-CSCF shall be co-located within the same network as the GGSN, which may reside in the VPLMN or HPLMN according to the APN and GGSN selection criteria, cf. TS 23.060 [10].

NOTE – The text in this specification applies to both IPsec and TLS-based access security unless otherwise noted.

P-CSCF in the Visited Network.

...

5.1 Secure access to IMS

5.1.1 Authentication of the subscriber and the network

...

The AKA-protocol is a secure protocol developed for UMTS and the same concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA.

NOTE – Although the method of calculating the parameters in UMTS AKA and IMS AKA are identical, the parameters are transported in slightly different ways. In UMTS, the UE's response RES is sent in the clear, while in IMS RES is not sent in the clear but combined with other parameters to form an authentication response and the authentication response is sent to the network (as described in RFC 3310 [17]).

An optional mechanism for authentication is SIP Digest. It is also a challenge response protocol, and operates in a similar manner to IMS AKA. An authentication vector containing authentication information is sent from the Home Stratum to the Serving Network. The serving network uses the authentication information in an authentication vector to authenticate the UE.

The Home Network authenticates the subscriber at anytime via the registration or re-registration procedures.

...

5.1.3 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation.

The following mechanisms are provided at SIP layer: for IPsec-based access security:

- 1) The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in clause 7.
- 2) The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1.

The following mechanisms are provided for TLS-based access security:

- 1) Negotiation of TLS related confidentiality protection features shall take place at the TLS layer as specified in clause 7.1.2.
- 2) The UE shall always offer TLS cipher suites for P-CSCF to be used for the session, as specified in RFC 2246 [31].
- 3) The P-CSCF shall decide whether the TLS cipher suites are used. If used, the UE and the P-CSCF shall agree on TLS cipher suites at the TLS layer as specified in RFC 2246 [31].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling, as specified in clause 6.3.

The following mechanisms are provided for IPsec-based access security:

- 1) The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session, as specified in clause 7.
- 2) The UE and the P-CSCF shall agree on security associations, which include the integrity keys, that shall be used for the integrity protection. The mechanism is based on IMS AKA and specified in clause 6.1.
- 3) The UE and the P-CSCF shall both verify that the data received originates from a node, which has the agreed integrity key. This verification is also used to detect if the data has been tampered with.
- 4) Replay attacks and reflection attacks shall be mitigated.

The following mechanisms are provided for TLS-based access security:

- 1) Negotiation of TLS-related integrity protection features shall take place at the TLS layer.
- 2) The use of TLS cipher suites with NULL integrity protection (or HASH) shall not be allowed.
- 3) The UE and the P-CSCF shall both verify that the data received originates from each other according to RFC 2246 [31]. This verification is also used to detect if the received data has been tampered with.
- 4) Replay attacks and reflection attacks shall be mitigated.

Integrity protection between CSCFs and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

NOTE 1 – TLS is mandatorily supported by SIP proxies according to RFC 3261 [6], and operators may use it to provide confidentiality and integrity inside their networks instead of or on top of IPsec, as the intra-domain Za interface is optional, and TLS may also be used between IMS networks on top of IPsec. It should be pointed out, that the 3GPP specifications do not provide support for TLS certificate management in a fashion similar to TS 33.310 (NDS/AF) [24] nor do they ensure backward compatibility with Release 5 CSCFs nor interoperability with other networks which do not use TLS, in case TLS is used by Release 6 CSCFs. These management and capability issues need then to be solved by manual configuration of the involved operators.

...

6.1 Authentication and key agreement

~~The~~ One scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. figure 1. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. TS 23.228 [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

~~The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS.~~ The security parameters e.g., keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in TS 33.102 [1]. The ISIM and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in TS 33.102 [1]. The AMF field can be used in the same way as in TS 33.102 [1].

An additional scheme for authentication is SIP Digest as specified in RFC 3261 [6]. SIP Digest achieves mutual authentication between the UE and the HN. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI. The HSS and the UE share a