

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**J.366.8**

(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



International  
Telecommunication  
Union

Documents  
Document Sharing Hub



# ITU-T Recommendation J.366.8

## IP-Cablecom2 IP Multimedia Subsystem (IMS): Network domain security specification

### Summary

This Recommendation introduces a new IP-Cablecom2 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/>.

© ITU 2007

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, symbols and abbreviations.....                                              | 1        |
|          | 3.1 Definitions.....                                                                     | 1        |
|          | 3.2 Symbols.....                                                                         | 1        |
|          | 3.3 Abbreviations .....                                                                  | 2        |
| 4        | Overview over UMTS network domain security for IP based protocols .....                  | 2        |
|          | 4.1 Introduction.....                                                                    | 2        |
|          | 4.2 Protection at the network layer .....                                                | 2        |
|          | 4.3 Security for native IP-based protocols .....                                         | 2        |
|          | 4.4 Security domains.....                                                                | 2        |
|          | 4.5 Security Gateways (SEGs).....                                                        | 2        |
| 5        | Key management and distribution architecture for NDS/IP.....                             | 2        |
|          | 5.1 Security services afforded to the protocols.....                                     | 2        |
|          | 5.2 Security Associations (SAs) .....                                                    | 2        |
|          | 5.3 Profiling of IPsec .....                                                             | 3        |
|          | 5.4 Profiling of IKE .....                                                               | 3        |
|          | 5.5 Security policy granularity.....                                                     | 3        |
|          | 5.6 UMTS key management and distribution architecture for native IP based protocols..... | 3        |
| <u>6</u> | <u>TLS Option for Protection of Intra-Network SIP .....</u>                              | <u>4</u> |
|          | <u>6.1 TLS Authentication Algorithms.....</u>                                            | <u>4</u> |
|          | <u>6.2 Key Exchange Algorithms for TLS .....</u>                                         | <u>4</u> |
|          | <u>6.3 Random Number Generator for TLS .....</u>                                         | <u>4</u> |
|          | <u>6.4 TLS Encryption Algorithms.....</u>                                                | <u>5</u> |
|          | <u>6.5 Ciphersuites for TLS.....</u>                                                     | <u>5</u> |
|          | <u>6.6 TLS Authentication.....</u>                                                       | <u>5</u> |
|          | <u>6.7 TLS Certificate Profile.....</u>                                                  | <u>6</u> |
|          | <u>6.8 Certificate Validation.....</u>                                                   | <u>6</u> |
|          | <u>6.9 Certificate Revocation.....</u>                                                   | <u>6</u> |
|          | Annexes A-D.....                                                                         | 7        |