

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.9

(11/2006)

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

IPCablecom

**IPCablecom2 IP Multimedia Subsystem (IMS):
Generic authentication architecture
specification**

ITU-T Recommendation J.366.9



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T Recommendation J.366.9

IPCablecom2 IP Multimedia Subsystem (IMS): Generic authentication architecture specification

Summary

This Recommendation describes the security features and a mechanism to bootstrap authentication and key agreement for application security.

Source

ITU-T Recommendation J.366.9 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
1.1	Relationship between IPCablecom 2.0 and 3GPP IMS.....	1
1.2	Scope of the present Recommendation	1
2	References.....	1
3	Definitions, abbreviations symbols and conventions	2
3.1	Definitions	2
3.2	Abbreviations	2
3.3	Symbols	2
3.4	Conventions.....	2
4	Generic Bootstrapping Architecture	2
4.1	Reference model	2
4.2	Network elements	2
4.3	Bootstrapping architecture and reference points	3
4.4	Requirements and principles for bootstrapping.....	4
4.5	Procedures	5
5	UICC-based enhancements to Generic Bootstrapping Architecture (GBA_U)	6
6	HTTP Digest Over TLS enhancements to Generic Bootstrapping Architecture (GBA_H)	6
6.1	Bootstrapping procedure	6
6.2	Procedures using bootstrapped Security Association	8
	Annex A – Void	10
	Annex B (normative) – Specification of the key derivation function KDF.....	10
	B.2 Generic key derivation function	10
	B.3 NAF specific key derivation in GBA ₁ and GBA_U, and GBA_H	10
	Annex C (informative) – Void	11
	Annex D (informative) – Dialog example for user selection of UICC application used in GBA.....	11
	Annex E (normative) – TLS profile for securing Zn' reference point	12
	Annex F (informative) – Handling of TLS certificates.....	12
	Annex G (normative) – GBA_U UICC-ME interface	12
	Annex H (normative) – Ua security protocol identifier.....	12

1