

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1197

(04/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection

Recommendation ITU-T X.1197



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1197

Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection

Summary

Recommendation ITU-T X.1197 provides guidelines on the criteria for selecting cryptographic algorithms for IPTV service and content protection (SCP). It also provides a list of cryptographic algorithms to provide confidentiality, data origin authentication and integrity for IPTV SCP services.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1197	2012-04-13	17

Keywords

Block cipher, cryptographic algorithm.

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 2012

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Terms and definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 Overview	3
6.1 General principles.....	3
6.2 1997 OECD guidelines for cryptography policy [b-OECD].....	3
6.3 EC Directives (directives of the European Parliament and of the Council)...	4
7 Requirements for cryptographic algorithms in IPTV	4
7.1 General requirements for cryptographic algorithms in [ITU-T X.1191]	4
7.2 Specific requirements of cryptographic algorithms for IPTV SCP.....	5
8 Criteria for selecting cryptographic algorithms for IPTV SCP	5
8.1 Security.....	5
8.2 Performance.....	5
8.3 Licensing issues.....	6
8.4 Maturity of cryptographic algorithms	6
8.5 Degree of endorsement.....	6
8.6 Level of adoption of a cryptographic algorithm.....	6
8.7 Number of cryptographic algorithms	6
Appendix I – Examples of possible cryptographic algorithms for the application of the criteria in clause 8 of this Recommendation.....	7
Appendix II – Examples of cryptographic algorithms for SRTP, IPSec and TLS protocols ..	9
Appendix III – OECD cryptography guidelines	11
Appendix IV – EC Directives	13
Bibliography.....	15

Recommendation ITU-T X.1197

Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection

1 Scope

Recommendation ITU-T X.1197 provides guidelines on the criteria for selecting cryptographic algorithms for IPTV service and content protection (SCP). It also provides a list of cryptographic algorithms to provide confidentiality, data origin authentication, and integrity for IPTV SCP services.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in the text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.
- [ITU-T Y.1911] Recommendation ITU-T Y.1911 (2010), *IPTV services and nomadism: Scenarios and functional architecture for unicast delivery*.
- [ISO/IEC 18033-1] ISO/IEC 18033-1 (2005), *Information technology – Security techniques – Encryption algorithms – Part 1: General*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 asymmetric encryption system [b-ISO/IEC 9798-1]: System based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption.

3.1.2 block cipher [ISO/IEC 18033-1]: Symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e., a string of bits of a defined length, to yield a block of ciphertext.

3.1.3 cipher [ISO/IEC 18033-1]: Alternative term for encryption system.

3.1.4 ciphertext [b-ITU-T X.800]: Data produced through the use of encipherment. The semantic content of the resulting data is not available.

NOTE – Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.

3.1.5 cryptanalysis [b-ITU-T X.800]: The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data, including cleartext.

3.1.6 encryption [b-ITU-T X.800]: See encipherment.

3.1.7 encipherment [b-ITU-T X.800]: The cryptographic transformation of data (see cryptography) to produce ciphertext.

NOTE – Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

3.1.8 encryption system [ISO/IEC 18033-1]: Cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys.

3.1.9 plaintext [ISO/IEC 18033-3]: Unenciphered information.

3.1.10 scrambling [ITU-T X.1191]: Process designed to protect multimedia content; scrambling usually uses encryption technology to protect content.

3.1.11 scrambling algorithm [ITU-T X.1191]: Algorithm used in a scrambling or a descrambling process.

3.1.12 service and content protection (SCP) [ITU-T X.1191]: A combination of service protection and content protection or the system or implementation thereof.

3.1.13 symmetric encryption system [ISO/IEC 18033-1]: Encryption system based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cryptographic algorithm suite: A set of cryptographic algorithms and relevant cryptographic parameters used for encryption, integrity protection, message origin authentication, key establishment, and non-repudiation, as well as corresponding key sizes and other parameters.

3.2.2 cryptographic methods: Cryptographic techniques, services, systems, products and key management systems.

3.2.3 cryptography: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation and/or prevent its unauthorized use.

NOTE – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.2.4 security strength: A measure of the difficulty of discovering the key in bits.

4 Abbreviations and acronyms

CBC	Cipher Block Chaining
ECB	Electronic Code Book
EC	European Commission
IPTV	Internet Protocol Television
OECD	Organization for Economic Co-operation and Development
OFB	Output Feedback mode
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission