International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1197

Amendment 1

(09/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (1) – IPTV security

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

Amendment 1

Recommendation ITU-T X.1197 (2012) – Amendment 1

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

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

Amendment 1

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.

Amendment 1 updates Appendices I and II to reflect the state of the art as of August 2019, including bibliographical references.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1197	2012-04-13	17	11.1002/1000/11582
1.1	ITU-T X.1197 (2012) Amd. 1	2019-09-05	17	11.1002/1000/14046

Keywords

Block cipher, cryptographic algorithm.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Recommendation ITU-T X.1197

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

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment have been introduced in clean text in the pdf version of the amendment, and are shown in revision marks relative to Recommendation ITU-T X.1197 (2012) in the Word file.

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

SCP Service and Content Protection

SDO Standards Development Organization

SRTP Secure Real-Time Transport Protocol

TLS Transport Layer Protocol

5 Conventions

The recommendation levels for Table I.1 and Table II.1 are represented by the following words:

RECOMMENDED: This word means that the definition is a valid current choice of a cryptographic algorithm, even against quantum attacks, providing that the chosen key length meets the requirements in Table I.2.

DEPRECATED: This word means that the definition is a possible choice of a cryptographic algorithm and is probably going to be removed from the list of recommendations within time. This can, for example, be an algorithm which is being kept in the table because it is still widely used but its security level does not offer a high buffer against serious threats anymore.

OBSOLETE: This word indicates that the algorithm should be removed from ITU-T X.1197, unless it is intended to mention negative examples.

For a direct comparison, the keywords from [b-IETF-BCP14] for use in IETF RFCs to indicate requirement levels include:

MUST, REQUIRED, SHALL: These words mean that the definition is an absolute requirement of the specification. They translate to *RECOMMENDED*.

MUST NOT, SHALL NOT: These phrases mean that the definition is an absolute prohibition of the specification. They translate to *OBSOLETE*.

SHOULD, RECOMMENDED: These words mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. This is translated to *RECOMMENDED*.

SHOULD NOT, NOT RECOMMENDED: These phrases mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label. These words translate to *OBSOLETE*.

MAY, OPTIONAL: These words mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. Additionally, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

6 Overview

6.1 General principles

The following principles should be applied when determining the criteria for selecting cryptographic algorithms for ITU-T IPTV SCP systems:

- Existing criteria that have been developed by ITU-T and other standards development organizations (e.g., ISO/IEC JTC 1/SC 27 and IETF) are used when determining the criteria.
- Based on the security strength and the selection criteria described in clause 8 of this Recommendation, cryptographic algorithms for IPTV SCP system are selected from:
  - publically available cryptographic algorithms that have been standardized [ISO/IEC JTC 1/SC 27];
  - cryptographic algorithms with a low computational complexity and a small carbon footprint, if applicable.

6.2 1997 OECD guidelines for cryptography policy [b-OECD]

On 27 March 1997, the Council of the OECD recommended guidelines for a cryptography policy [b-OECD]. Cryptographic algorithms include algorithms for encryption, message authentication and key derivation algorithms. The guidelines were primarily aimed at governments, in terms of policy recommendations, but with anticipation that they would be widely read and followed by both the private and public sectors. Since each of the eight principles outlined in the OECD guidelines addresses an important policy concern, they should be implemented as a whole to balance the various interests at stake.

Among the eight principles outlined in the OECD guidelines, four are of importance in the selection of cryptographic algorithms for IPTV SCP:

1. Trust in cryptographic methods
2. Choice of cryptographic methods
3. Market driven development of cryptographic methods
4. Standards for cryptographic methods.

These four principles are extracted from the guidelines included in Appendix III.

6.3 EC Directives (directives of the European Parliament and of the Council)

A set of EC communication directives, intended to harmonize electronic communication regulation throughout the European community, forms the basis for the European regulatory regime. Among the set of EC Directives covering the area of electronic communications, the following two are of importance from a regulatory perspective, in the selection of cryptographic algorithms for the IPTV SCP:

1. Universal Service Directive (Directive 2002/22/EC)
2. Access Directive (Directive 2002/19/EC).

These Directives were amended on 25 November 2009.

The Universal Service Directive addresses the question of interoperability of digital consumer equipment in Article 24, in conjunction with Annex VI, which refers to the common European scrambling algorithm.

The Access Directive adds aspects of conditional access systems, addressing in Article 6, the implementation of measures by the European Commission and the responsibilities of national

regulatory authorities. The Access Directive also includes, in conjunction with Annex I, further conditions for conditional access systems.

The text referring to these two EC Directives can be found in Appendix IV of this Recommendation.

7 Requirements for cryptographic algorithms in IPTV

7.1 General requirements for cryptographic algorithms in [ITU-T X.1191]

The general requirements and/or recommendations, described in [ITU-T X.1191], can be applied for selecting the cryptographic algorithm:

Requirements for scrambling algorithms

- Scrambling algorithms for a broadcast stream are required to support the periodic update of the necessary cryptographic keys.
- Scrambling algorithms for IPTV are required to be built using publicly available and standardized cryptographic algorithms.

Recommendations for scrambling algorithms

- Scrambling algorithms for IPTV are recommended to have sufficiently large key entropy to effectively protect the content from crypt-analysis.
- The IPTV architecture is not prohibited from precluding support for widely used scrambling algorithms.
- The IPTV architecture is recommended to refrain from precluding support for multiple scrambling systems.
- Scrambling algorithms for IPTV are recommended to be efficiently implementable for both hardware and/or software implementations.
- Scrambling algorithms for IPTV are recommended to be scalable and future-proof, i.e., cryptographic parameters (e.g., key length, crypto periods, etc.) or cryptographic mode (e.g., CBC, OFB, ECB, etc.).
- The IPTV architecture is recommended to support multiple scrambling algorithms.

Options for scrambling algorithms

- Scrambling algorithms for IPTV can optionally apply cryptographic algorithms of varying strength to different content types.

Key management

- The IPTV architecture is required to support the capability to update and query the SCP system concerning the scrambling algorithms for IPTV, and any other operator-selected scrambling algorithm on the server side via SCP interfaces.

7.2 Specific requirements of cryptographic algorithms for IPTV SCP

- Cryptographic algorithms for IPTV SCP are required to have security strength (i.e., key strength) with at least 112 bits [b-SP 800-131].
- Cryptographic algorithms for IPTV SCP are required to be selected based on the selection criteria described in clause 8.
- In order to verify evidence of the correctness of implementation of cryptographic algorithms, the following four deliverables are recommended to be provided: a specification of the algorithms; a set of design conformance test data; a set of algorithm input/output test data and a design and evaluation report.

- The design and evaluation report is recommended to provide to potential users of the algorithm, specification and test data, to provide evidence of the correctness of implementation of cryptographic algorithms.
- The evaluation report should explain the algorithm and test data design criteria, the algorithm evaluation criteria, the methodology used to design and evaluate the algorithm; the extent of the mathematical analysis and statistical testing applied to the algorithm, the principal conclusions of the algorithm evaluation and the quality control applied to the production of the algorithm specification and test data, the algorithm specification and test data.
- An unambiguous specification of the algorithm is required to be provided which is suitable for use by implementers of the algorithm.
- Design conformance test data is required to allow implementers of the algorithm to test their implementations.
- Algorithm input/output test data is required to allow users of the algorithm to test the algorithm as a "blackbox" function.
- It is recommended to provide to the users of the algorithm with the confidence that it is fit for the purpose by providing deliverables described above, and to provide users and implementers of the algorithm with the assurance that appropriate quality control has been exercised in their production.

8 Criteria for selecting cryptographic algorithms for IPTV SCP

8.1 Security

The security of cryptographic algorithms must be resistant to all known crypt-analysis attacks, that is, selected algorithms must be resistant to cryptanalytic attack, differential analysis, linear analysis, algebraic analysis, etc. The existence of a proof of security is regarded as a significant argument in favour of a cipher, depending on the security model and the proof assumptions. The nature of any evaluation is of great importance, especially if it is conducted by widely recognized evaluation organizations.

8.2 Performance

The performance of cryptographic algorithms on a variety of platforms includes not only time and space efficiency, but also demonstrates whether or not it possesses the characteristics that give advantages over other cryptographic algorithms. It is recommended to consider if algorithms are power-efficient for use in, noting also any constraints of low power devices.

8.3 Licensing issues

The licensing issues of cryptographic algorithms do not affect implementation.

8.4 Maturity of cryptographic algorithms

The maturity of cryptographic algorithms is evaluated in terms of the extent to which they are used, the level to which they have been examined, and how widely any analysis has been published.

8.5 Degree of endorsement

It refers to the degree to which cryptographic algorithms are advocated by a recognized organization (e.g., a standards development body, a government agency, etc.), or whether they are under investigation and/or analysis for endorsement by such a body. It also includes the degree to which the cryptographic algorithm is used in the market.

8.6 Level of adoption of a cryptographic algorithm

The cryptographic algorithms that are de-facto algorithms are to be favoured over less well-used techniques.

8.7 Number of cryptographic algorithms

The number of cryptographic algorithms should be as small as possible, to help the implementer in the selection of the appropriate algorithm for his application.

Appendix I

Examples of possible cryptographic algorithms for the application of the criteria in clause 8 of this Recommendation

(This appendix does not form an integral part of this Recommendation.)

While using multiple encryption and message authentication, algorithms for IPTV SCP may not be precluded. Some examples are given in this appendix for the application of the criteria in clause 8. Table I.1 describes examples of cryptographic algorithms for IPTV SCP.

Table I.1 – Examples of possible cryptographic algorithms for IPTV SCP

Classification		Status	Algorithms
Digest		RECOMMENDED [b-IETF RFC 8247]: MUST	SHA-3 [b-FIPS PUB 202]
			SHA-256/384/512 [b-IETF RFC 6234]
		DEPRECATED [b-NIST IR 8105]	RIPEMD-160 [b-IETF RFC 2286]
Message authentication		RECOMMENDED [b-IETF RFC 8247]: MUST	HMAC-SHA-256/384/512 [b-IETF RFC 4868]
		RECOMMENDED [b-IETF RFC 8247]: MUST	HMAC-SHA1 [b-IETF RFC 6151]
Digital signature		RECOMMENDED	XMSS [b-IETF RFC 8391] and LMS [b-IETF RFC 8554]
		DEPRECATED *[b-NIST IR 8105]* Important note from [b-IETF RFC 8247]: SHOULD be kept for interoperability	RSA [b-ISO/IEC 18033-2]
			DSA [b-ISO 14888-3]
		DEPRECATED *[b-NIST IR 8105]* Important note from [b-IETF RFC 8247]: SHOULD be used with SHA-256 on P-256 curve with SHA-384 on P-384 curve with SHA-512 on P-521 curve	ECDSA [b-ISO 14888-3]
		DEPRECATED [b-NIST IR 8105]	KCDSA [b-ISO 14888-3]
Symmetric cipher		RECOMMENDED [b-NIST IR 8105] [b-IETF RFC 8247]: MUST (AES256)	AES256 [b-ISO/IEC 18033-3]
			Camellia256 [b-ISO/IEC 18033-3]
			ARIA256 [b-IETF RFC 5794]
		DEPRECATED *[b-NIST IR 8105]*	SEED [b-ISO/IEC 18033-3]
			Camellia128/192, ARIA128/192, AES128/192
			HIGHT [b-ISO/IEC 18033-3]
Asymmetric cipher	Encryption	DEPRECATED *[b-NIST IR 8105]*	RSA [b-ISO/IEC 18033-2]
			ECC [b-IETF RFC 5753]

Table I.1 – Examples of possible cryptographic algorithms for IPTV SCP

Classification		Status	Algorithms
	Encryption and key exchange	RECOMMENDED (Note 1)	NTRU [b-IEEE 1363.1-2008]
	Key exchange	DEPRECATED (Note 2) *[b-NIST IR 8105]* Note to implementers: Check valid DH-Groups in [b-IETF RFC 8247] 2.4. Type 4 – IKEv2 Diffie-Hellman Group Transforms!	DH [b-IETF RFC 2136]
			ECDH [b-IETF RFC 6090]
NOTE 1 – With the caveat that currently only pre-shared keys can prevent Man-in-the-Middle attacks [b-MitM-NTRU-KE]. NOTE 2 – [b-ACM] and [b-NIST IR 8105] - *u*se physical key distribution when possible. NOTE 3 – See clause 5 for the conventions used in the status column.			

Table I.2 describes safety of the key and its lengths supported in IPTV SCP.

Table I.2 – Key length properties [b-SP 800-131]

Property			Key length
Symmetric key	Minimum length (deprecated, [b-NIST IR 8105])		128
	Minimum quantum-safe length [b-NIST IR 8105]		256
	Maximum length [b-NIST IR 8105]		512
Asymmetric key	RSA (deprecated, [b-NIST IR 8105])	Minimum length (Note 1)	2048
		Maximum length	4096
	EC DH (deprecated, [b-NIST IR 8105])	Minimum length (Note 2)	224
		Maximum length	512
	NTRU	Minimum security level [b-NIST-round2-PQC-NTRU] and [b-ISO/IEC 18033-1]	n = 509 and q = 2048 (providing ca. 128-bit equivalent security level in classical model)
		Maximum security level [b-NIST-round2-PQC-NTRU] and [b-ISO/IEC 18033-1]	n = 821 and q = 4096 (providing ca. 256-bit equivalent security level in classical model)
NOTE 1 – Safe until 2030 according to NIST estimation back in 2013 [b-Pockock-RSA]. NOTE 2 – 224-bit EC ≈ 2048-bit RSA.			

Appendix II

Examples of cryptographic algorithms for SRTP, IPSec and TLS protocols

(This appendix does not form an integral part of this Recommendation.)

Table II.1 of Appendix II describes the cryptographic algorithms for SRTP, IPSec and TLS protocols specified by IETF.

Table II.1 – Typical cryptographic algorithms for SRTP, IPSec and TLS protocol

Protocols	RFC	Title	Algorithms
SRTP	[b-IETF RFC 3711]	The Secure Real-time Transport Protocol	AES[a)], HMAC-SHA1
	[b-IETF RFC 5669]	The SEED Cipher Algorithm and Its Use with the Secure Real-time Transport Protocol (SRTP)	SEED, HMAC-SHA1
IPSec	[b-IETF RFC 4308]	Cryptographic Suites for IPSec	AES-128[a)], HMAC-SHA1 XCBC-MAC
	[b-IETF RFC 8423]	Reclassification of Suite B Documents to Historic Status[b)]	AES-128[a)], AES-256, SHA-256, SHA-384 HMAC-SHA-256, HMAC-SHA-384, ECDSA-256[c)], ECDSA-384[c)]
	[b-IETF RFC 4196]	The SEED Cipher Algorithm and Its Use with IPSec	SEED-128[a)], HMAC-SHA1
	[b-IETF RFC 4312]	The Camellia Cipher Algorithm and its Use with IPSec	Camellia-128[a)]/192[a)]/256
TLS	[b-IETF RFC 5246]	The TLS Protocol Version 1.2	AES-128[a)]. AES-256, HMAC-SHA1, SHA-256
	[b-IETF RFC 4162]	Addition of SEED Cipher Suites to Transport Layer Security (TLS)	SEED-128[a)], HMAC-SHA1
	[b-IETF RFC 4132]	Addition of Camellia Cipher Suites to Transport Layer Security (TLS)	Camellia-128[a)]/256, HMAC-SHA1

Table II.1 – Typical cryptographic algorithms for SRTP, IPSec and TLS protocol

Protocols	RFC	Title	Algorithms
	[b-IETF RFC 5430]	Suite B Profile for Transport Layer Security (TLS)	AES-128[a)], AES-256, HMAC-SHA1, SHA256, SHA384

a) For symmetric algorithms, those with key size < 256 bits are deprecated by [b-NIST IR 8105].

b) For updated guidance on the use of (deprecated) elliptic-curve algorithms for IKEv2, see [b-IETF RFC 8247], in particular section 2.4. Type 4 – IKEv2 Diffie-Hellman Group Transforms.

c) Due to the quantum threat, whenever possible, use pre-shared keys (e.g., through physical means) or NTRU [b-IEEE 1363.1-2008] with parameters from [b-NIST-round2-PQC-NTRU] instead of ECDSA-based key exchange, to ensure long-term content protection, with the caveat that currently, only pre-shared keys can prevent Man-in-the-Middle attacks [b-MitM-NTRU-KE].

A complete cryptographic suite, suitable for power-constrained embedded systems, is widely deployed in various forms and parameter settings: ZigBee Smart Energy 1.0 with 25 million devices, IEEE 1609.2 (vehicle to vehicle), and ISA SP100.11a (industrial automation).

Appendix III

OECD cryptography guidelines

(This appendix does not form an integral part of this Recommendation.)

Appendix III describes the principles selected from the OECD cryptographic guidelines [b-OECD] that are related to the selection criteria for cryptographic algorithms for IPTV SCP.

- **Trust in cryptographic methods**

Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communication systems. Market forces should serve to build trust in reliable systems, government regulation, and licensing. Use of cryptographic methods and evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust. In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

- **Choice of cryptographic methods**

Users should have the right to choose any cryptographic method, subject to applicable law. Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communication systems, and in the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data, may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfil different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs. In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection. Government controls on cryptographic methods should be no more than those essential to the discharge of government responsibilities, and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.

- **Market-driven development of cryptographic methods**

Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments. The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users, and evolving threats to information and communication systems security. The development of international technical standards, criteria, and protocols related to cryptographic methods, should also be market-driven. Governments should encourage and co-operate with the business and research communities in the development of cryptographic methods.

- **Standards for cryptographic methods**

Technical standards, criteria, and protocols for cryptographic methods, should be developed and promulgated at the national and international level. In response to market needs, internationally recognized standards-making bodies, governments, business, and other relevant experts, should share information and collaborate to develop and promulgate interoperable technical standards, criteria, and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such technical standards, criteria, and protocols for interoperability, portability and mobility of cryptographic methods, should be developed. To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should be encouraged.

Appendix IV

EC Directives

(This appendix does not form an integral part of this Recommendation.)

Appendix IV reproduces text quoted from EC Directive 202/EC (2002) [b-EC-22:2002] and EC Directive 192/EC (2002) [b-EC-19:2002], that are relevant to selection guidelines for cryptographic algorithms for IPTV SCP.

Universal Service Directive (USD) 2002/22/EC, [b-EC-22:2002] Annex VI, Interoperability of digital consumer equipment referred to in Article 24:

1. Common scrambling algorithm and free-to-air reception

All consumer equipment intended for the reception of conventional digital television signals (i.e. broadcasting via terrestrial, cable or satellite transmission which is primarily intended for fixed reception, such as DVB-T, DVB-C or DVB-S), for sale or rent or otherwise made available in the Community, capable of descrambling digital television signals, is to possess the capability to:

- *allow the descrambling of such signals according to a common European scrambling algorithm as administered by a recognised European standards organisation, currently ETSI,*
- *display signals that have been transmitted in the clear provided that, in the event that such equipment is rented, the renter is in compliance with the relevant rental agreement.*

• • •

Access Directive 2002/19/EC [b-EC-19:2002], Article 6, Conditional access systems and other facilities:

1. Member States shall ensure that, in relation to conditional access to digital television and radio services broadcast to viewers and listeners in the Community, irrespective of the means of transmission, the conditions laid down in Annex I, Part I apply.

• • •

Annex I of the Access Directive is further taken into account as follows:

Annex I Conditions for access to digital television and radio services broadcast to viewers and listeners in the Community:

***Part I**: Conditions for conditional access systems to be applied in accordance with Article 6(1)*

In relation to conditional access to digital television and radio services broadcast to viewers and listeners in the Community, irrespective of the means of transmission, Member States must ensure in accordance with Article 6 that the following conditions apply:

(a) conditional access systems operated on the market in the Community are to have the necessary technical capability for cost-effective transcontrol allowing the possibility for full control by network operators at local or regional level of the services using such conditional access systems;

(b) *all operators of conditional access services, irrespective of the means of transmission, who provide access services to digital television and radio services and whose access services broadcasters depend on to reach any group of potential viewers or listeners are to:*

- *offer to all broadcasters, on a fair, reasonable and non-discriminatory basis compatible with Community competition law, technical services enabling the broadcasters' digitally-transmitted services to be received by viewers or listeners authorised by means of decoders administered by the service operators, and comply with Community competition law,*
- *keep separate financial accounts regarding their activity as conditional access providers.*

(c) *when granting licenses to manufacturers of consumer equipment, holders of industrial property rights to conditional access products and systems are to ensure that this is done on fair, reasonable and non-discriminatory terms. Taking into account technical and commercial factors, holders of rights are not to subject the granting of licenses to conditions prohibiting, deterring or discouraging the inclusion in the same product of:*

- *a common interface allowing connection with several other access systems, or*
- *means specific to another access system, provided that the licensee complies with the relevant and reasonable conditions ensuring, as far as he is concerned, the security of transactions of conditional access system operators.*

…

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-IETF-BCP14] IETF RFC 2119, BCP 14 (1997), *Key words for use in RFCs to Indicate Requirement Levels*.

[b-IETF RFC 2286] IETF RFC 2286 (1998), *Test Cases for HMAC-RIPEMD160 and HMAC-RIPEMD128*.

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

[b-IETF RFC 4162] IETF RFC 4162 (2005), *Addition of SEED Cipher Suites to Transport Layer Security (TLS)*.

[b-IETF RFC 4196] IETF RFC 4196 (2005), *The SEED Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use With IPsec*.

[b-IETF RFC 4868] IETF RFC 4868 (2007), *Using HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 with IPsec*.

[b-IETF RFC 4869] IETF RFC 4869 (2007), *Suite B Cryptographic Suites for IPsec*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5430] IETF RFC 5430 (2009), *Suite B Profile for Transport Layer Security (TLS)*.

[b-IETF RFC 5669] IETF RFC 5669 (2010), *The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)*.

[b-IETF RFC 5753] IETF RFC 5753 (2010), *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 6090] IETF RFC 6090 (2011), *Fundamental Elliptic Curve Cryptography Algorithms*.

[b-IETF RFC 6151] IETF RFC 6151 (2011), *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*.

[b-IETF RFC 6234] IETF RFC 6234 (2011), *US Secure Hash Algorithms* (SHA and SHA-based HMAC and HKDF).

[b-IETF RFC 8247] IETF RFC 8247, *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*.

[b-IETF RFC 8391] IETF RFC 8391 (2018), *XMSS: eXtended Merkle Signature Scheme*.

[b-IETF RFC 8554] IETF RFC 8554 (2019), *Leighton-Micali Hash-Based Signatures*.

[b-EC-22:2002] Directive 2002/22/EC (2002), on *Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)*.

[b-EC-19:2002] Directive 2002/19/EC (2002), on *Access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)*.

[b-ISO/IEC 9798-1] ISO/IEC 9798-1 (1997), *Information technology – Security techniques – Entity authentication – Part 1: General*.

[b-ISO/IEC 10116] ISO/IEC 10116 (1997), *Information technology – Security techniques – Modes of operation for an n-bit block cipher*.

[b-ISO 14888-3] ISO 14888-3 (2006), *Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*.

[b-ISO/IEC 18033-1] ISO/IEC 18033-1, *Information technology – Security techniques – Encryption algorithms – Part 1: General*.

[b-ISO/IEC 18033-2] ISO/IEC 18033-2 (2006), *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.

[b-ISO/IEC 18033-3] ISO/IEC 18033-3 (2010), *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

[b-ISO/IEC SHA-1] ISO/IEC JTC 1/SC 27 (2017), *JTC 1/SC 27 statement of SHA-1*. <https://www.din.de/blob/236540/5b946078899f420e2b15fb64e3ca3e17/20170425-sc-27-statement-of-sha-1-data.pdf>

[b-ACM] D. Adrian, K. Bhargavan et al., Communications of the ACM, 2019. *Imperfect Forward Secrecy: How Diffie-Hellmann Fails in Practice*.

[b-CERT-MD5] Carnegie Mellon University, Software Engineering Institute (2008), *MD5vulnerable to collision attacks*. <https://www.kb.cert.org/vuls/id/836068 31/12/2008>

[b-FIPS PUB 202] National Institute of Standards and Technology, Federal Information Processing Standards 202 (2015), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*.

[b-NIST IR 8105] National Institute of Standards and Technology Interagency Report 8105 (2016), *Report on Post-Quantum Cryptography*. <https://csrc.nist.gov/publications/detail/nistir/8105/final>

[b-NIST-PQC-NTRU] National Institute of Standards and Technology, *NIST Post-Quantum Competition, round 2 entry for NTRU*. <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/NTRU-Round2.zip>

[b-NIST-Sweet32] National Institute of Standards and Technology, *NIST Moves on Sweet32 – 3DES, Blowfish, and Others – Mostly Unsafe*. <https://controlgap.com/blog/nist-moves-on-sweet32/>

[b-OECD] OECD (1997), *Cryptography Policy: The guidelines and the issues (the OECD cryptography policy guidelines and the report on background and issues of cryptography policy)*.

[b-Pockock-RSA] Website - Daniel Pockock (2013), *RSA Key Sizes: 2048 or 4096 bits?* <https://danielpocock.com/rsa-key-sizes-2048-or-4096-bits>

[b-SHA-1_Kcrypt18] *From Collisions to Chosen-Prefix Collisions: Application to Full SHA-1*. T.Peyrin, Kangacrypt'18. <https://www.kangacrypt.info/program.php#TP>

[b-SP 800-131] National Institute of Standards and Technology, NIST SP 800-131 (2010), *Recommendation for the transitioning of cryptographic algorithms and key sizes*.

[b-SWEET32] K. Bhargavan, G. Leurent, ACM CCS 2016, *On the Practical (In-)Security of 64-bit Block Ciphers – Collision Attacks on HTTP over TLS and OpenVPN*.
<https://sweet32.info/SWEET32_CCS16_slides.pdf >

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019