INTERNATIONAL STANDARD

ISO/IEC 15444-8

Second edition
2023-10

Information technology — JPEG 2000 image coding system —

Part 8: Secure JPEG 2000

Technologies de l'information — Système de codage d'images JPEG 2000 —

Partie 8: JPEG 2000 sécurisé

Reference number
ISO/IEC 15444-8:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T (as ITU-T Rec T.807) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

This second edition cancels and replaces the first edition (ISO/IEC 15444-8:2007), which has been technically revised. It also incorporates the Amendment ISO/IEC 15444-8:2007/Amd 1:2008.

A list of all parts in the ISO/IEC 15444 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

INTERNATIONAL STANDARD ISO/IEC 15444-8
RECOMMENDATION ITU-T T.807

Information technology – JPEG 2000 image coding system: Secure JPEG 2000

Summary

Rec. ITU-T T.807 | ISO/IEC 15444-8 provides a syntax that allows security services to be applied to JPEG 2000 coded image data. Security services include confidentiality, integrity verification, source authentication, conditional access, secure scalable streaming and secure transcoding. The syntax allows these security services to be applied to coded and uncoded image data in part or in its entirety. This maintains the inherent features of JPEG 2000 such as scalability and access to various spatial areas, resolution levels, colour components, and quality layers, while providing security services on these elements.

This second edition:

1) consolidates all solved/outstanding amendments and corrigenda published since the first edition;
2) removes the clause on Registration Authority (first edition's clause 7);
3) removes the annex of patent statements (first edition's Annex D).

This Recommendation | International Standard was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information,* in collaboration with ITU-T SG16. The identical text is published in ISO/IEC as ISO/IEC 15444-8.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T T.807	2006-05-29	16	11.1002/1000/8830
1.1	ITU-T T.807 (2006) Amd. 1	2008-03-15	16	11.1002/1000/9364
2.0	ITU-T T.807 (V2)	2023-02-13	16	11.1002/1000/15208

Keywords

Image security, jpsec, JPEG 2000, security, still image.

* 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.

© ISO/IEC 2023 – All rights reserved

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2023

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

© ISO/IEC 2023 – All rights reserved

CONTENTS

Page

1 Scope ... 1
2 Normative references ... 1
3 Definitions ... 1
4 Symbols and abbreviations ... 4
5 JPSEC syntax ... 5
5.1 JPSEC framework overview ... 5
5.2 JPSEC security services ... 6
5.3 Comments on design and implementation of secure JPSEC systems ... 7
5.4 Byte aligned segment (BAS) ... 8
5.5 Main security marker (SEC) ... 9
5.6 JPSEC tools ... 13
5.7 Zone of Influence (ZOI) syntax ... 16
5.8 Protection method template syntax (T) ... 25
5.9 Processing domain syntax (PD) ... 34
5.10 Granularity syntax (G) ... 35
5.11 Value list syntax (V) ... 36
5.12 Relationships among ZOI, Granularity (G) and Value List (VL) ... 37
5.13 In-codestream security marker (INSEC) ... 38
6 Normative-syntax usage examples (informative) ... 39
6.1 ZOI examples ... 39
6.2 Key information template examples ... 43
6.3 JPSEC normative tool examples ... 44
6.4 Distortion field examples ... 50
Annex A Guidelines and use cases ... 52
A.1 A class of JPSEC applications ... 52
Annex B Interoperability ... 58
B.1 Rec. ITU-T T.800 | ISO/IEC 15444-1 – Core coding system ... 58
B.2 Rec. ITU-T T.808 | ISO/IEC 15444-9 – JPIP ... 58
B.3 Rec. ITU-T T.810 | ISO/IEC 15444-11 – JPWL ... 59
Annex C File format security ... 62
C.1 Scope ... 62
C.2 Introduction ... 62
C.3 Extension to ISO base media file format ... 64
C.4 Elementary stream and sample definitions ... 72
C.5 Protection at file format level ... 74
C.6 Examples (Informative) ... 75
C.7 Boxes defined in ISO/IEC 14496-12 (informative) ... 85
Annex D Technology examples ... 90
D.1 Introduction ... 90
D.2 A flexible access control scheme for JPEG 2000 codestreams ... 90
D.3 A unified authentication framework for JPEG 2000 images ... 92
D.4 A simple packet-based encryption method for JPEG 2000 codestreams ... 94
D.5 Encryption tool for JPEG 2000 access control ... 97
D.6 Key generation tool for JPEG 2000 access control ... 99
D.7 Wavelet and bitstream domain scrambling for conditional access control ... 102
D.8 Progressive access for JPEG 2000 codestream ... 104
D.9 Scalable authenticity of JPEG 2000 codestreams ... 106
D.10 JPEG 2000 data confidentiality and access control system based on data splitting and luring ... 108
D.11 Secure scalable streaming and secure transcoding ... 111
Bibliography ... 115

© ISO/IEC 2023 – All rights reserved

FIGURES

Page

Figure 1 – Overview of the conceptual steps in JPSEC framework 5
Figure 2 – Byte aligned segment (BAS) structure 8
Figure 3 – Main security marker segment syntax 9
Figure 4 – Main security marker syntax when multiple marker segments are used 10
Figure 5 – Codestream security parameters (P_{SEC}) syntax 10
Figure 6 – TRLCP tag descriptor (P_{TRLCP}) syntax 11
Figure 7 – Use of multiple JPSEC tools 12
Figure 8 – JPSEC tool syntax ($Tool^{(i)}$) 13
Figure 9 – Parameters (P_{ID}) syntax for JPSEC normative tools (t = 0) 14
Figure 10 – ID_{RA} syntax 15
Figure 11 – Zone of Influence conceptual structure 17
Figure 12 – ZOI syntax 17
Figure 13 – Zone description class structure (DCzoi) 18
Figure 14 – Zone syntax consists of a description class and one or more parameter sets 18
Figure 15 – Distortion field syntax 20
Figure 16 – Distortion field syntax 21
Figure 17 – Relative importance field syntax 21
Figure 18 – Bit-rate field syntax 22
Figure 19 – ZOI example using image related descriptions 23
Figure 20 – ZOI example using image related and non-image related descriptions 23
Figure 21 – A second ZOI example using image related and non-image related descriptions 24
Figure 22 – ZOI description parameter syntax 24
Figure 23 – Decryption template syntax 26
Figure 24 – Block cipher template syntax 27
Figure 25 – Stream cipher template syntax 28
Figure 26 – Asymmetric cipher template syntax 29
Figure 27 – Authentication template syntax 29
Figure 28 – Hash-based authentication template 30
Figure 29 – Cipher-based authentication template syntax 31
Figure 30 – Digital signature template syntax 32
Figure 31 – Hash template syntax 33
Figure 32 – Key information template syntax 33
Figure 33 – ITU-T X.509 certificate syntax 34
Figure 34 – Processing domain syntax 34
Figure 35 – Granularity syntax 35
Figure 36 – Value list field syntax 37
Figure 37 – Granularity Level (GL) is resolution 37

© ISO/IEC 2023 – All rights reserved

Page

Figure 38 – Granularity Level (GL) is layer 38
Figure 39 – In-codestream security marker syntax 38
Figure A.1 – Overview of a secure JPEG 2000 image distribution application 52
Figure A.2 – Legend description 53
Figure A.3 – Encryption procedure 54
Figure A.4 – Decryption procedure 54
Figure A.5 – Signature generation procedure 55
Figure A.6 – Authentication procedure 56
Figure A.7 – ICV generation procedure 56
Figure A.8 – Integrity check procedure 57
Figure B.1 – Typical JPWL and JPSEC combination 60
Figure C.1 – System diagram for time-sequenced scalable media 63
Figure C.2 – Self-contained ES and scalable composed ES 73
Figure C.3 – Self-contained ES and decodable composed ES 73
Figure C.4 – Relationship between iloc, iinf and ipro 74
Figure C.5 – An example sample description entry protected by authentication scheme followed by description scheme 75
Figure C.6 – Example 1: Item-based protection of JP2 file (authentication) 76
Figure C.7 – Example 2: Item-based protection of a JPEG 2000 images (encryption) 77
Figure C.8 – Example 2: Secure transcoding to lower resolution (discarding resolution 2) 77
Figure C.9 – Example 3: Item-based protection of a JPEG 2000 image (Authentication) 78
Figure C.10 – Example 3: Transcoding to resolution 1 79
Figure C.11 – Example 4: Sample-based protection of a time-sequenced JPEG 2000 pictures 80
Figure C.12 – Example 4: Secure transcoding to lower SNR quality (layer 1) 81
Figure C.13 – Example 5: Sample-based protection for video browsing or video summarization 82
Figure C.14 – Example 5: Transcoding to shorter time length (discarding the last 5000 pictures) 82
Figure C.15 – Example 6: Authentication transcoding, discarding received but unverifiable packets 83
Figure C.16 – Motion JPEG 2000 file with detailed box structure 83
Figure C.17 – Simplified Motion JPEG 2000 box structure showing references 84
Figure C.18 – Simplified Motion JPEG 2000 box structure showing references after length changing protection operations 84
Figure C.19 – JPM file with detailed box structure 85
Figure C.20 – Simplified JPM box structure showing references 85
Figure C.21 – JPM box structure showing references after length changing protection operations 85
Figure D.1 – SEC segment syntax 91
Figure D.2 – P_{ID} field syntax 91
Figure D.3 – TP_{ID} field syntax 91
Figure D.4 – AK_{info} field syntax 92
Figure D.5 – Image protection using unified authentication framework for JPEG 2000 93

© ISO/IEC 2023 – All rights reserved

Page

Figure D.6 – Packet-based encryption principle 95
Figure D.7 – Overview of this technology 100
Figure D.8 – Block diagram for wavelet domain scrambling 102
Figure D.9 – Block diagram for bitstream domain scrambling 103
Figure D.10 – Non-normative protection tool syntax in the case of multiple keys 103
Figure D.11 – Syntax for AP: Wavelet domain scrambling (left), Bitstream domain scrambling (right) 104
Figure D.12 – Technical overview of this technology 105
Figure D.13 – Non-normative tool syntax 107
Figure D.14 – Security parameters TP_{ID} syntax 108
Figure D.15 – System overview 110
Figure D.16 – JPSEC enables end-to-end security and mid-network secure transcoding 112
Figure D.17 – An example of forming a JPSEC codestream 113

TABLES

Page

Table 1 – Main security parameter values 10
Table 2 – Codestream security parameters (P_{SEC}) in first SEC marker segment 11
Table 3 – Semantics for F_{PSEC} values (FBAS) 11
Table 4 – Parameter field for TRLCP tag descriptor (P_{TRLCP}) 12
Table 5 – JPSEC tool parameter values 13
Table 6 – JPSEC normative tool Template ID values (ID_T) 14
Table 7 – JPSEC normative tool parameter values 15
Table 8 – Parameters values in ID_{RA} syntax 15
Table 9 – ID values for JPSEC non-normative tools ($ID_{RA,id}$) 16
Table 10 – Zone of influence field (ZOI) parameter values 17
Table 11 – Zone parameter values 18
Table 12 – Description class indicator value 18
Table 13 – Image related description class 18
Table 14 – Non-image related description class 19
Table 15 – Distortion field parameter values 20
Table 16 – Distortion field parameter values 21
Table 17 – Relative importance field parameter values 21
Table 18 – Bit-rate field parameter values 22
Table 19 – $Pzoi^i$ parameter values 24
Table 20 – Mzoi parameter values 25
Table 21 – Template ID values (ID_T) 25
Table 22 – Decryption template parameter values 26
Table 23 – Marker emulation flag values (ME_{decry}) 26

© ISO/IEC 2023 – All rights reserved

Page

Table 24 – Cipher identifier values (CT_{decry}) ... 26
Table 25 – Block cipher identifier values (CT_{decry}) ... 26
Table 26 – Stream cipher identifier values (CT_{decry}) ... 27
Table 27 – Asymmetric cipher identifier values (CT_{decry}) ... 27
Table 28 – Block cipher template values ... 27
Table 29 – Block cipher mode values (M_{bc}) ... 28
Table 30 – Padding mode for block cipher (P_{bc}) ... 28
Table 31 – Stream cipher template values ... 28
Table 32 – Asymmetric cipher template values ... 29
Table 33 – Authentication template parameter values ... 29
Table 34 – Authentication methods (M_{auth}) ... 29
Table 35 – Hash-based authentication template parameter values ... 30
Table 36 – Hash-based authentication method identifier (M_{HMAC}) ... 30
Table 37 – Hash function identifier (H_{HMAC}) ... 31
Table 38 – MAC template values ... 31
Table 39 – Cipher-based authentication method (C_{CMAC}) ... 32
Table 40 – Digital signature template values ... 32
Table 41 – Digital signature methods (M_{DS}) ... 32
Table 42 – Hash template parameter values ... 33
Table 43 – Key template values ... 33
Table 44 – Key information identifier values (KID_{KT}) ... 34
Table 45 – ITU-T X.509 certificate values (KI_{KT} if $KID_{KT} = 2$) ... 34
Table 46 – Encoding rule values (ER_{KT}) ... 34
Table 47 – Processing domain parameters ... 35
Table 48 – Processing Domain (PD) parameter values ... 35
Table 49 – Processing domain field (F_{PD}) parameter values in wavelet coefficient domain and quantized wavelet coefficient domain ... 35
Table 50 – Processing domain field (F_{PD}) parameter values in codestream domain ... 35
Table 51 – Granularity parameter values (G) ... 36
Table 52 – Processing order values (PO) ... 36
Table 53 – Granularity level values (GL) ... 36
Table 54 – Value list field (V) parameter values ... 37
Table 55 – In-codestream security parameter values (INSEC) ... 39
Table 56 – Relevance zone values (R) ... 39
Table 57 – ZOI in example 1 ... 39
Table 58 – ZOI in example 2 ... 40
Table 59 – ZOI in example 3 ... 41
Table 60 – ZOI in example 4 ... 41
Table 61 – ZOI in example 5 ... 42

© ISO/IEC 2023 – All rights reserved

Page

Table 62 – ZOI in example 6 ... 43
Table 63 – Key information in example 1 ... 43
Table 64 – Key information in example 2 ... 43
Table 65 – Key information in example 3 ... 44
Table 66 – Key information in example 4 ... 44
Table 67 – SEC marker segment for example 1 ... 45
Table 68 – ZOI example ... 45
Table 69 – P_{ID} example ... 46
Table 70 – Decryption template example ... 47
Table 71 – Key template example ... 47
Table 72 – The SEC marker segment ... 48
Table 73 – ZOI signalling ... 48
Table 74 – P_{ID} signalling parameters ... 49
Table 75 – Associating distortion field to two data segments (extension of ZOI example 3 in 6.1.3) ... 50
Table 76 – Signalling a range of packets and associating distortions for each packet ... 51
Table C.1 – List of existing and new boxes ... 64
Table D.1 – Example parameters for this scheme ... 91
Table D.2 – P_{ID} parameters ... 91
Table D.3 – TP_{ID} parameters ... 92
Table D.4 – AK_{info} parameters ... 92
Table D.5 – Syntax for semi-fragile authentication ... 93
Table D.6 – Example of Zone of Influence, with spatial coordinates, resolutions and layers ... 95
Table D.7 – Decryption template description, in the case of AES-192/CBC ... 96
Table D.8 – Processing domain syntax ... 96
Table D.9 – Granularity and value list syntax ... 97
Table D.10 – Example parameters for this technology ... 98
Table D.11 – Example ZOI of this key generation tool ... 98
Table D.12 – P_{ID} for this technology ... 99
Table D.13 – Example of decryption template of this technology ... 99
Table D.14 – Recommended parameter in this technology ... 100
Table D.15 – Example ZOI of this key generation tool ... 101
Table D.16 – P_{ID} for this technology ... 101
Table D.17 – Example of decryption template of this technology ... 102
Table D.18 – Syntax and semantic for P_{ID} ... 103
Table D.19 – Syntax and semantic for AP ... 104
Table D.20 – Example parameters for this tool ... 105
Table D.21 – Example ZOI of this technology ... 106
Table D.22 – P_{ID} for this technology ... 106

© ISO/IEC 2023 – All rights reserved

Page

Table D.23 – Example of decryption template of this technology 106
Table D.24 – Non-normative tool parameters 108
Table D.25 – Security parameters..... 108
Table D.26 – Parameter values for this tool 111
Table D.27 – Parameter values for template protection tool, processing domain and granularity 114
Table D.28 – Parameter values for authentication template protection tool..... 114

© ISO/IEC 2023 – All rights reserved

Introduction

In the "Digital Age", the Internet provides many new opportunities for right-holders regarding the electronic distribution of their work (books, videos, music, images, etc.).

At the same time, new information technology radically simplifies the access of content for the user. This goes hand in hand with the all-pervasive problem of pirated digital copies – with the same quality as the originals – and "file-sharing" in peer-to-peer networks, which gives rise to continued complaints about great losses by the content industry.

World Intellectual Property Organization (WIPO) and its Member countries (170) have an important role to play in assuring that copyright, and the cultural and intellectual expression it fosters, remains well protected in the 21st century. The new Digital economy and the creative people in every country of the world depend on it. Also in December 1996, WIPO Copyright Treaty (WCT) has been promulgated with two important articles (11 and 12) about technological measures and obligations concerning Right Management Information:

Article 11
Obligations concerning
Technological Measures

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Article 12
Obligations concerning Rights
Management Information

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

This treaty provides a solid foundation to protect Intellectual Property. As of 2004, about 50 countries ratified this important treaty. Therefore, it is expected that tools and protective methods that are recommended in JPEG 2000 needs ensure the security of transaction, protection of content (IPR), and protection of technologies.

Security issues, such as authentication, data integrity, protection of copyright and Intellectual Property, privacy, conditional access, confidentiality, transaction tracing, to mention a few, are among important features in many imaging applications targeted by JPEG 2000.

The technological means of protecting digital content are described and can be achieved in many ways such as digital watermarking, digital signature, encryption, metadata, authentication, and integrity checking.

This Recommendation | International Standard intends to provide tools and solutions in terms of specifications that allow applications to generate, consume, and exchange Secure JPEG 2000 codestreams. This is referred to as **JPSEC**.

© ISO/IEC 2023 – All rights reserved

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – JPEG 2000 image coding system: Secure JPEG 2000

1 Scope

This Recommendation | International Standard specifies the framework, concepts, and methodology for securing JPEG 2000 codestreams. The scope of this Recommendation | International Standard is to define:

1) a normative codestream syntax containing information for interpreting secure image data;
2) informative examples of JPSEC tools in typical use cases;
3) informative guidelines on how to implement security services and related metadata.

The scope of this Recommendation | International Standard is not to describe specific secure imaging applications or to limit secure imaging to specific techniques, but to create a framework that enables future extensions as secure imaging techniques evolve.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. At the time of publication, the editions indicated in dated references were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

- Recommendation ITU-T T.800 | ISO/IEC 15444-1, *Information technology – JPEG 2000 image coding system: Core coding system*.
- Recommendation ITU-T T.801 | ISO/IEC 15444-2, *Information technology – JPEG 2000 image coding system: Extensions*.
- Recommendation ITU-T T.808 | ISO/IEC 15444-9, *Information technology – JPEG 2000 image coding system: Interactivity tools, APIs and protocols.*
- Recommendation ITU-T T.814 | ISO/IEC 15444-15, *Information technology – JPEG 2000 image coding system: High-Throughput JPEG 2000.*
- Recommendation ITU-T X.509 | ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ISO/IEC 14496-12, *Information technology* – Coding of audio-visual objects – *Part 12: ISO base media file format*.

3 Definitions

For the purposes of this document, the definitions contained in Rec. ITU-T T.800 | ISO/IEC 15444-1, Rec. ITU-T T.801 | ISO/IEC 15444-2, Rec. ITU-T T.808 | ISO/IEC 15444-9, Rec. ITU-T T.814 | ISO/IEC 15444-15, and ISO/IEC 14496-12, and the following apply.

3.1 access control: Prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.2 adaptive-format decoder: Process to decode a codestream which is not fully compliant with the normative part of the coding standard.

NOTE – It reconstructs the media (possibly with low quality or resolution) even if the codestream has missing packets or inconsistent packet headers. For example, an adaptive-format decoder is able to understand a simply transcoded codestream, such as the one that has its highest resolution packets removed.

3.3 adaptor/transcoder: process to transform media data to lower scalability level, like lower resolution or lower quality or bit-rate, by removing portions of the file.

© ISO/IEC 2023 – All rights reserved