

ISO/IEC 15444-8:2023-10 (E)

Information technology - JPEG 2000 image coding system - Part 8: Secure JPEG 2000

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

FIGURES

	<i>Page</i>
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

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

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

	<i>Page</i>
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 TRLC _P tag descriptor (P _{TRLC_P})	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

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

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

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