NORME INTERNATIONALE

ISO/CEI 15444-8

Première édition
2007-04-15

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

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

Numéro de référence
ISO/CEI 15444-8:2007(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2008

Publié en Suisse

TABLE DES MATIÈRES

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 15444-8 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 29, *Codage du son, de l'image, de l'information multimédia et hypermédia* en collaboration avec l'UIT-T. Le texte identique est publié en tant que Rec. UIT-T T.807.

L'ISO/CEI 15444 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Système de codage d'images JPEG 2000*:

— *Partie 1: Système de codage de noyau*

— *Partie 2: Extensions*

— *Partie 3: Images JPEG 2000 animées*

— *Partie 4: Tests de conformité*

— *Partie 5: Logiciel de référence*

— *Partie 6: Format de fichier d'image de composant*

— *Partie 8: JPEG 2000 sécurisé*

— *Partie 9: Outils d'interactivité, interfaces de programmes d'application et protocoles*

— *Partie 10: Extensions pour données tridimensionnelles*

— *Partie 11: Communications sans fil*

— *Partie 12: Format ISO de base pour les fichiers médias*

La partie suivante est en préparation:

— *Partie 13: Un encodeur JPEG 2000 de niveau d'entrée*

Introduction

A "l'ère numérique", le réseau Internet offre aux ayants droit de nombreuses et nouvelles opportunités concernant la distribution électronique de leurs œuvres (livres, films, partitions musicales, images, etc.).

En même temps, de nouvelles technologies de l'information simplifient radicalement l'accès aux contenus par les utilisateurs. Cela va de pair avec le problème généralisé des copies numériques piratées – avec la même qualité que l'original – et avec celui du "partage de fichiers" dans les réseaux d'homologue à homologue, ce qui engendre des plaintes récurrentes, concernant de grandes pertes, de la part de l'industrie des contenus.

L'Organisation mondiale de la propriété intellectuelle (OMPI) et ses (170) pays Membres ont un important rôle à jouer afin de garantir que le droit d'auteur, ainsi que l'expression culturelle et intellectuelle qu'il suscite, restera bien protégé au cours du 21e siècle. La nouvelle économie numérique et les créateurs de chaque pays du monde en dépendent. C'est pourquoi, en décembre 1996, le Traité de l'OMPI sur le droit d'auteur (WCT) a été promulgué avec deux importants articles (11 et 12) sur les obligations relatives aux mesures techniques et aux informations sur le régime des droits:

Article 11

Obligations relatives aux mesures techniques

Les Parties contractantes doivent prévoir une protection juridique appropriée et des sanctions juridiques efficaces contre la neutralisation des mesures techniques efficaces qui sont mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits en vertu du présent traité ou de la Convention de Berne et qui restreignent l'accomplissement, à l'égard de leurs œuvres, d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi.

Article 12

Obligations relatives aux informations sur le régime des droits

(1) Les Parties contractantes doivent prévoir des sanctions juridiques appropriées et efficaces contre toute personne qui accomplit l'un des actes suivants en sachant, ou, pour ce qui relève des sanctions civiles, en ayant des raisons valables de penser que cet acte va entraîner, permettre, faciliter ou dissimuler une atteinte à un droit prévu par le présent traité ou la Convention de Berne:

(i) supprimer ou modifier, sans y être habilitée, toute information relative au régime des droits se présentant sous forme électronique;

(ii) distribuer, importer aux fins de distribution, radiodiffuser ou communiquer au public, sans y être habilitée, des œuvres ou des exemplaires d'œuvres en sachant que des informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifiées sans autorisation.

(2) Dans le présent article, l'expression "les informations sur le régime des droits" s'entend des informations permettant d'identifier l'œuvre, l'auteur de l'œuvre, le titulaire de tout droit sur l'œuvre ou des informations sur les conditions et modalités d'utilisation de l'œuvre, et de tout numéro ou code représentant ces informations, lorsque l'un quelconque de ces éléments d'information est joint à l'exemplaire d'une œuvre ou apparaît en relation avec la communication d'une œuvre au public.

Ce traité fournit une base solide afin de protéger la propriété intellectuelle. En 2004, une cinquantaine de pays avaient ratifié cet important traité. L'on s'attend donc que les outils et méthodes de protection qui sont recommandés dans le système JPEG 2000 ne manqueront pas d'assurer la sécurité des transactions, la protection des contenus (droits de propriété intellectuelle (IPR, Intellectual Property Rights)) et la protection des technologies.

Les questions de sécurité telles que l'authentification, l'intégrité des données, la protection du droit d'auteur et de la propriété intellectuelle, la protection de la sphère privée, l'accès conditionnel, la confidentialité, le suivi des transactions, pour n'en mentionner que quelques-unes, font partie des caractéristiques importantes dans de nombreuses applications d'imagerie visées par le système JPEG 2000.

Les moyens techniques permettant de protéger un contenu numérique sont décrits et peuvent être réalisés par de nombreux procédés tels que le filigranage numérique, la signature numérique, le chiffrement, les données métalinguistiques (métadonnées), l'authentification et la vérification d'intégrité.

La présente Partie 8 de la norme JPEG 2000 vise à offrir des outils et des solutions en termes de spécifications permettant aux applications de produire, de consommer et d'échanger des flux à codage JPEG 2000 sécurisé. C'est ce qui est désigné par le terme de **syntaxe JPSEC**.

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information – Système de codage d'images JPEG 2000: JPEG 2000 sécurisé

1 Domaine d'application

La présente Recommandation | Norme internationale spécifie le cadre, les concepts et les méthodes permettant de sécuriser les flux à codage JPEG 2000. Le domaine d'application de la présente Recommandation | Norme internationale consiste à définir:

1) une syntaxe normative de flux codé contenant des informations permettant d'interpréter des données d'image sécurisées;
2) un processus normatif permettant d'enregistrer des outils JPSEC auprès d'un organisme d'enregistrement délivrant un identificateur unique;
3) des exemples informatifs d'outils JPSEC dans des cas de figure typiques;
4) des directives informatives sur la façon de mettre en œuvre des services de sécurité et les métadonnées associées.

Le domaine d'application de la présente Recommandation | Norme internationale ne vise pas à décrire des applications spécifiques d'imagerie sécurisée ni à limiter l'imagerie sécurisée à des techniques spécifiques, mais à créer un cadre autorisant de futures extensions au fur et à mesure de l'évolution des techniques d'imagerie sécurisée.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT (TSB) tient à jour une liste des Recommandations de l'UIT-T en vigueur.

– Recommandation UIT-T T.800 (2002) | ISO/CEI 15444-1:2004, *Technologies de l'information – Système de codage d'images JPEG 2000: Système de codage noyau*.

– Recommandation UIT-T T.801 (2002) | ISO/CEI 15444-2:2004, *Technologies de l'information – Système de codage d'images JPEG 2000: Extensions*.

3 Termes et définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent. Les définitions données dans la Rec. UIT-T T.800 | ISO/CEI 15444-1, § 3, s'appliquent à la présente Recommandation | Norme internationale.

3.1 **contrôle d'accès**: prévention d'un usage non autorisé d'une ressource, y compris la prévention de l'utilisation d'une ressource de façon non autorisée.

3.2 **authentification**: processus de vérification d'une identité revendiquée par ou pour une entité systémique.

3.2.1 **authentification de la source**: vérification du fait qu'une entité d'origine (p. ex. un utilisateur/correspondant) est réellement l'entité d'origine revendiquée.

3.2.2 **authentification d'image fragile/semi-fragile**: processus visant à la fois l'authentification d'image de la source et la vérification de l'intégrité des données ou du contenu d'image, qui devrait être en mesure de détecter toute

modification du signal et de déterminer où cette modification a eu lieu, en précisant éventuellement quelle était la nature du signal avant sa modification.

NOTE – Ce processus sert à prouver l'authenticité d'un document. La différence entre authentification fragile et authentification semi-fragile d'une image est que la première consiste à vérifier l'intégrité des données d'image et la seconde à vérifier l'intégrité du contenu d'image.

3.3 **confidentialité**: propriété par laquelle des informations ne sont pas mises à la disposition ni révélées à des individus, entités ou processus non autorisés.

3.4 **découpage des données**: méthode visant à protéger des données sensibles contre un accès non autorisé en chiffrant ces données et en mémorisant différentes portions du fichier dans différents serveurs distants.

NOTE – Quand des données découpées font l'objet d'un accès, les parties sont extraites, combinées et déchiffrées. Une personne non autorisée aurait besoin de connaître les emplacements des serveurs contenant les parties, d'être en mesure d'avoir accès à chaque serveur, de savoir quelles sont les données à combiner et de savoir comment les déchiffrer.

3.5 **déchiffrement**: transformation inverse du chiffrement

3.6 **signature numérique**: donnée adjointe à une unité de données – ou transformation cryptographique de cette unité – qui permet à un destinataire de cette unité de données d'en prouver l'origine et l'intégrité, et qui permet de la protéger contre une création frauduleuse, p. ex. par son destinataire.

3.7 **chiffrement**: transformation réversible de données par un algorithme cryptographique afin de produire un cryptogramme, c'est-à-dire afin de masquer le contenu informationnel des données.

NOTE – Un synonyme du terme *algorithme de chiffrement* est: *chiffre*.

3.8 **empreinte digitale**: caractéristique d'un objet qui tend à distinguer d'autres objets similaires afin de permettre à son propriétaire de retrouver la trace d'utilisateurs autorisés les distribuant illégalement.

NOTE – A cet égard, la prise d'empreintes digitales est habituellement analysée dans le contexte du problème de la recherche criminelle.

3.9 **fonction de hachage**: fonction qui fait correspondre des chaînes de bits à des chaînes de bits de longueur fixe en répondant aux deux conditions suivantes.

NOTE – Pour une sortie donnée, il est mathématiquement impossible de trouver une entrée qui mappe à cette sortie; pour une entrée donnée, il est mathématiquement impossible de trouver une seconde entrée qui mappe à la même sortie. La faisabilité mathématique dépend des exigences de sécurité propres à l'utilisateur et à son environnement.

3.10 **intégrité**: propriété d'être en mesure de sauvegarder la précision et la complétude de ressources.

3.10.1 **intégrité des données d'image**: propriété par laquelle des données n'ont pas été altérées ni détruites de façon non autorisée.

3.10.2 **intégrité du contenu d'image**: assurance que le contenu d'image n'a pas été modifié par des utilisateurs non autorisés au point de modifier la perception de sa signification.

NOTE – Cette propriété permet d'appliquer à l'image des opérations de protection du contenu sans déclencher l'alarme d'intégrité.

3.11 **application JPSEC**: tout processus logiciel ou matériel qui est capable de consommer des flux à codage JPSEC en interprétant la syntaxe JPSEC afin d'offrir les services de sécurité spécifiés.

NOTE – Une application JPSEC fait usage d'un ou de plusieurs outils JPSEC.

EXEMPLE – Une application JPSEC sera en mesure de lire des flux JPSEC codés et chiffrés, de les déchiffrer si la clé appropriée lui a été fournie et de restituer sans codage les données d'image JPEG 2000 originales.

3.12 **flux à codage JPSEC**: séquence de bits résultant du codage et de la sécurisation d'une image au moyen du codage JPEG 2000 et des outils de sécurité JPSEC.

3.12.1 **créateur JPSEC**: entité qui crée un flux à codage JPSEC à partir d'une image, d'un flux à codage JPEG 2000, ou d'un autre flux à codage JPSEC afin d'offrir certains services JPSEC.

3.12.2 **consommateur JPSEC**: entité qui reçoit un flux à codage JPSEC et qui rend un service JPSEC fondé sur le flux codé.

3.13 **service JPSEC**: service qui protège la consommation d'images à codage JPEG 2000. Ce service déjoue les attaques compromettant la sécurité et fait usage d'un ou de plusieurs outils JPSEC.

3.14 **organisme d'enregistrement JPSEC**: entité chargée de délivrer un identificateur unique afin de faire référence à un outil JPSEC et chargée de mémoriser la liste des paramètres contenus dans la description d'outil JPSEC.

3.15 **outil JPSEC**: processus matériel ou logiciel qui utilise des techniques de sécurité afin de mettre en œuvre un service de sécurité

3.15.1 outil JPSEC normatif: outil JPSEC qui utilise des modèles d'outil prédéfinis pour le déchiffrement, pour l'authentification ou pour le hachage comme spécifié par la partie normative de la présente Recommandation | Norme internationale.

3.15.2 outil JPSEC non normatif: outil JPSEC spécifié par un numéro d'identification attribué par l'organisme d'enregistrement JPSEC ou par une application définie par l'utilisateur.

3.15.3 outil JPSEC défini par l'utilisateur: outil JPSEC non normatif qui est défini par une application définie par l'utilisateur.

3.15.4 outil JPSEC défini par l'organisme d'enregistrement: outil JPSEC non normatif qui est défini par l'organisme d'enregistrement JPSEC.

3.16 description d'outil JPSEC: description des paramètres utilisés par l'outil JPSEC.

NOTE – La description d'outil JPSEC ne décrit toutefois pas l'algorithme ou la méthode que l'on utilise. Une description d'outil JPSEC se compose de deux parties: la liste des paramètres et ses valeurs. Dans le cas d'outils JPSEC normatifs, la liste des paramètres est donnée par la norme. Dans le cas d'outils JPSEC non normatifs, la liste des paramètres peut être fournie par l'organisme d'enregistrement. Dans les deux cas, les valeurs paramétriques sont spécifiées dans les segments marqueurs SEC et INSEC.

3.17 clé: séquence de symboles qui commande les opérations de chiffrement et de déchiffrement.

3.17.1 clés symétriques: paire de clés pour lesquelles aussi bien l'expéditeur que le destinataire utilisent la même clé secrète ou deux clés qui peuvent être facilement calculées, l'une à partir de l'autre, dans un système cryptographique.

3.17.2 paire de clés asymétriques: paire de clés associées où la clé privée définit la transformation privée et où la clé publique définit la transformation publique.

3.17.2.1 clé privée: clé faisant partie d'une paire de clés asymétriques d'entité, qui ne devrait pas être révélée.

3.17.2.2 clé publique: clé faisant partie d'une paire de clés asymétriques d'entité, qui peut être rendue publique.

3.18 production de clé, fonction de production de clé: fonction qui reçoit en entrée un certain nombre de paramètres dont au moins un doit être secret, et qui envoie en sortie des clés appropriées à l'algorithme et à l'application que l'on envisage.

NOTE – La fonction doit avoir la propriété qu'il doit être mathématiquement impossible de déduire la sortie sans connaissance préalable de l'entrée secrète.

3.19 gestion des clés: production, mémorisation, distribution, suppression, archivage et application de clés conformément à une politique de sécurité.

3.20 émulation de marqueur: cryptogramme résultant du processus de chiffrement, qui contient un code de déclenchement JPEG.

3.21 algorithme d'un code d'authentification de message, fonction de contrôle cryptographique, fonction de somme de contrôle cryptographique: algorithme permettant de calculer une fonction qui affecte des chaînes de bits et une clé secrète à des chaînes de bits de longueur fixe, en satisfaisant les deux propriétés suivantes:

- pour toute clé et toute chaîne d'entrée, la fonction peut être calculée efficacement;
- pour toute clé fixe, sans aucune connaissance préalable de la clé, il est mathématiquement impossible de calculer la valeur de la fonction d'après une quelconque nouvelle chaîne d'entrée, même avec la connaissance de l'ensemble des chaînes d'entrée et des valeurs correspondantes de la fonction, où la valeur de la ième chaîne d'entrée peut avoir été choisie après observation de la valeur des i-1 premières valeurs de la fonction.

NOTE – La faisabilité mathématique dépend des exigences de sécurité propres à l'utilisateur et de son environnement.

3.21.1 code d'authentification de message (code MAC, *message authentication code*): chaîne de bits qui est la sortie d'un algorithme de codage MAC.

3.22 non-répudiation: association d'une entité à une transaction à laquelle elle participe, de façon que cette transaction ne puisse pas être ultérieurement répudiée (refusée).

NOTE – C'est-à-dire que le récepteur d'une transaction est en mesure de démontrer à une tierce partie neutre que l'expéditeur revendiqué a effectivement envoyé la transaction.

3.23 paquet: partie du flux de bits conforme à la Partie 1 de la norme JPEG 2000, composée d'un en-tête de paquet et des données d'image comprimées extraites d'une couche donnée du district d'une composante de pavé donnée, à une résolution donnée.

NOTE – Ce terme possède un acception différente du terme "paquet" qui est utilisé en transmission de données dans un réseau.

3.24 protection: processus visant à sécuriser un contenu.

3.24.1 modèle de protection: champs de modèle ou de liste de paramètres, nécessaires au fonctionnement d'une méthode de protection.

3.24.1 méthode de protection: méthode servant à créer ou à consommer un contenu protégé, telle que le chiffrement, le déchiffrement, l'authentification et la vérification d'intégrité.

3.25 sécurité: tous les aspects contribuant à définir, à réaliser et à conserver la confidentialité, l'intégrité, la disponibilité, l'imputabilité, l'authenticité et la fiabilité.

NOTE – Un produit, système ou service est considéré comme étant sécurisé si ses utilisateurs peuvent partir du principe qu'il fonctionne (ou va fonctionner) de la façon prévue. La sécurité est habituellement considérée dans le contexte d'une évaluation de dangers, réels ou perçus comme tels.

3.26 syntaxe de signalisation: spécification du format du flux à codage JPSEC qui contient toutes les informations requises pour consommer des images à codage JPEG 2000 sécurisé.

3.27 transcodage: opération consistant à recevoir en entrée un flux codé comprimé et à l'adapter ou à le convertir afin d'émettre en sortie un flux codé comprimé qui possède une certaine propriété recherchée.

EXEMPLE – Le flux codé comprimé de sortie peut représenter une image avec une résolution spatiale inférieure ou avec un débit binaire inférieur au flux codé comprimé d'entrée.

3.27.1 transcodage sécurisé: opération consistant à exécuter le transcodage ou l'adaptation d'une entrée de contenu comprimé protégé sans compromettre cette protection.

NOTE – Le terme *transcodage sécurisé* est utilisé, par opposition à *transcodage*, afin de souligner le fait que l'opération de transcodage est effectuée sans compromettre la sécurité. Le transcodage sécurisé peut également être considéré comme l'exécution d'un transcodage dans le domaine cryptographique.

3.28 filigrane: signal imperceptiblement ajouté au signal de masquage afin d'acheminer des données masquées.

3.28.1 filigranage: processus qui insère imperceptiblement, dans des données multimédias de l'une des deux façons suivantes, des données représentant certaines informations:

- la méthode avec perte qui signifie que le signal de masquage exact ne pourra jamais être récupéré une fois le filigrane imbriqué;
- la méthode sans perte qui signifie que le signal de masquage exact pourra être récupéré après extraction du filigrane.

4 Symboles et abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent.

BAS	Segment verrouillé en octets (*byte aligned segment*)
FBAS	Segment verrouillé en octets d'un champ (*field byte aligned segment*)
G	Granularité
GL	Niveau de granularité (*granularity level*)
INSEC	Marqueur de sécurité de flux binaire entrant (*in-codestream security marker*)
IP	Propriété intellectuelle associée à une technologie (*intellectual property related to technology*)
IPR	Droits de propriété intellectuelle associés à un contenu (*intellectual property rights related to content*)
JPSEC	Codage JPEG 2000 sécurisé (*secure JPEG 2000*)
KT	Modèle de clé (*key template*)
LSB	Bit de plus faible poids (*least significant bit*)
MAC	Code d'authentification de message (*message authentication code*)
MSB	Bit de plus fort poids (*most significant bit*)
PD	Domaine de traitement (*processing domain*)
PKI	Infrastructure de clés publiques (*public key infrastructure*)
PO	Ordre de traitement (*processing order*)
RA	Organisme d'enregistrement (*registration authority*)
RBAS	Segment verrouillé en octets d'une étendue (*range byte aligned segment*)
SEC	Marqueur de sécurité (*security marker*)

T	Modèle (*template*)
V	Valeurs
VL	Liste de valeurs (*value list*)
ZOI	Zone d'influence

5 Syntaxe JPSEC (paragraphe normatif)

5.1 Aperçu général du cadre JPSEC

La syntaxe JPSEC définit un cadre pour la sécurisation de données à codage JPEG 2000. Le noyau de la présente Recommandation | Norme internationale est la spécification de la syntaxe de l'image à codage JPEG 2000 sécurisé: le *flux à codage JPSEC*. La syntaxe est orientée vers les données à codage JPEG 2000. Elle permet la protection de tout ou partie du flux codé. En toutes circonstances, les données protégées (c'est-à-dire les flux à codage JPSEC) doivent suivre la syntaxe normative définie dans la présente Recommandation | Norme internationale.

Au flux à codage JPSEC sont associés un certain nombre de *services de sécurité JPSEC*, y compris la confidentialité et l'authentification de l'origine et du contenu.

La syntaxe *de signalisation* spécifie:

- quels services de sécurité sont associés aux données d'image;
- quels *outils JPSEC* sont requis afin de fournir les services correspondants;
- comment les outils JPSEC sont appliqués;
- quelles parties des données d'image sont protégées.

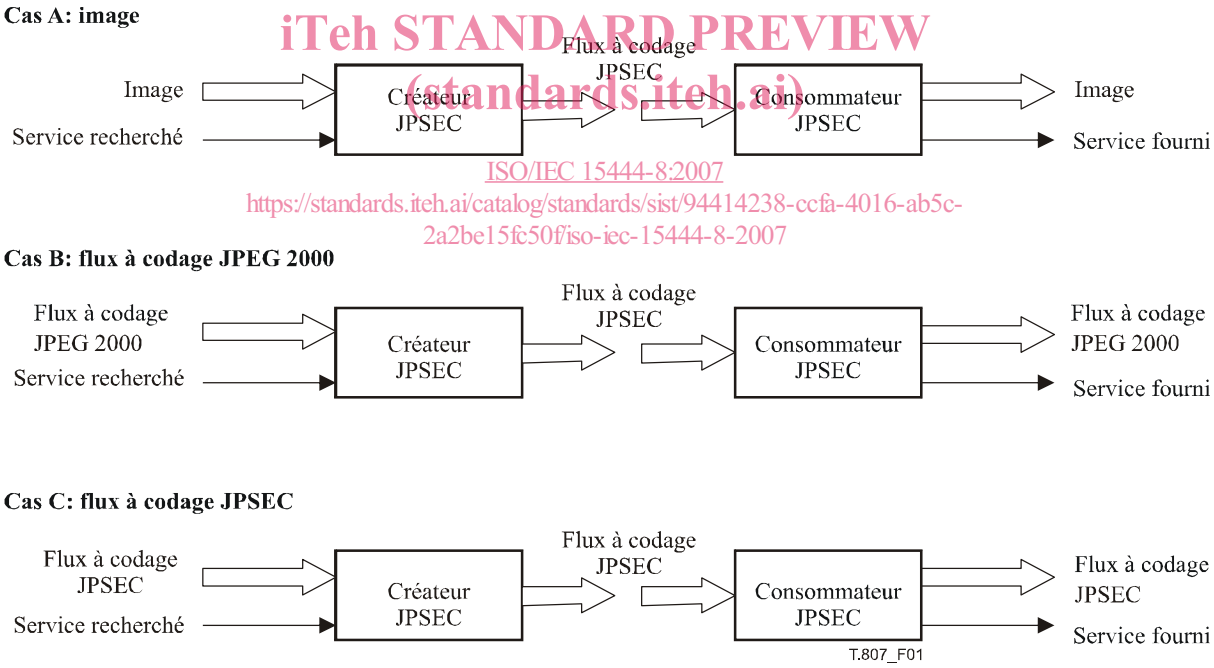

Figure 1 – Aperçu général des étapes théoriques dans le cadre JPSEC

La syntaxe du flux à codage JPSEC est normative. L'objectif consiste à permettre aux applications JPSEC de consommer des flux à codage JPSEC de façon interopérable (voir Figure 1): l'application consommatrice JPSEC interprète le flux à codage JPSEC, recherche et applique les outils JPSEC signalés, achemine les services correspondants de sécurité, puis transmet le flux ou l'image à codage JPEG 2000 pour traitement subséquent, p. ex. par un visionneur d'images.

Comme représenté dans le cas C de la Figure 1, le flux à codage JPSEC peut être créé à partir d'un autre flux à codage JPSEC. Cela peut se produire quand de multiples outils JPSEC sont appliqués au même contenu, mais à différents moments ou par différentes entités. Quand cela se produit, l'ordre dans lequel les outils JPSEC sont appliqués pendant les opérations de création et de consommation peut être significatif.

La syntaxe de signalisation identifie les outils qui sont utilisés par un consommateur JPSEC. Ces outils sont définis soit par la partie normative de la norme, ou par l'organisme d'enregistrement, ou par des outils privés. Les outils définis de façon normative prennent en charge la confidentialité (au moyen d'outils de chiffrement) ainsi que l'authentification de la source et du contenu. Ils autorisent le type le plus élevé d'interopérabilité car des implémentations indépendantes du processus de consommation sont en mesure de traiter le même flux à codage JPSEC et de rendre les services correspondants avec le même comportement.

La façon dont le flux à codage JPSEC est créé est hors du domaine d'application de la présente Recommandation | Norme internationale. Pour être conformes, les créateurs JPSEC doivent produire des flux à codage JPSEC qui comprennent la signalisation JPSEC appropriée. Des flux à codage JPSEC peuvent être créés d'un certain nombre de façons. Par exemple, un outil JPSEC peut être appliqué à des éléments d'image (pixels) ou à des coefficients d'ondelette, ou à des coefficients quantifiés, ou à des paquets.

Un consommateur peut implémenter un ou plusieurs outils JPSEC. Par exemple, il pourra exécuter un déchiffrement en utilisant l'analyse par blocs AES en mode ECB et une vérification de signature en utilisant le hachage SHA-128 et une clé publique RSA. Avec ces capacités, il sera capable d'exécuter des services de sécurité comme la confidentialité et l'authentification.

Dans le cadre de la syntaxe JPSEC, les outils JPSEC sont spécifiés par des modèles définis secrètement, ou sont enregistrés par un *organisme d'enregistrement JPSEC*. Les outils JPSEC spécifiés par les modèles ont un comportement de traitement unique et ne nécessitent donc pas d'identification unique. Ceux qui sont spécifiés par l'organisme d'enregistrement sont associés à un numéro unique d'identification fourni par le registre commun.

5.2 Services de sécurité JPSEC

L'objectif du présent paragraphe consiste à énumérer et à expliquer les fonctionnalités qui sont incluses dans le domaine d'application de la présente Recommandation | Norme internationale.

Les outils JPSEC servent à peut implémenter des fonctions de sécurité. La syntaxe JPSEC est un cadre ouvert, c'est-à-dire extensible dans le temps. Actuellement, il est centré sur les aspects suivants:

– *Confidentialité via chiffrement, sélectif ou non sélectif*

  Un fichier JPSEC peut prendre en charge une transformation de données non codées (image et/ou métadonnées) en une forme (cryptogramme) qui masque la signification originale de ces données. Par *chiffrement sélectif*, l'on entend que ce n'est pas la totalité, mais seulement des parties de l'image et/ou des métadonnées qui peuvent être chiffrées.

– *Vérification d'intégrité*

  Un fichier JPSEC peut prendre en charge des moyens permettant de détecter des manipulations apportées à l'image et/ou aux métadonnées et ainsi vérifier leur intégrité. Il y a deux classes de vérification de l'intégrité:

  1) vérification de l'intégrité des données d'image où même un seul bit de données d'image erroné se traduit par un échec de vérification (c'est-à-dire que la vérification renvoie le message: "pas d'intégrité"). Cette vérification est par ailleurs souvent désignée par le terme de *vérification fragile (d'intégrité) d'image*;

  2) vérification de l'intégrité du contenu d'image, où même une certaine altération occasionnelle des données d'image se traduit par un succès de vérification tant que cette altération ne change pas le contenu d'image du point de vue du système visuel humain ou, en d'autres termes, tant que la perception du sens de l'image ne change pas. Cette vérification est également souvent désignée par le terme de *vérification semi-fragile (d'intégrité) d'image*.

  Cette vérification fragile ou semi-fragile de l'intégrité pourrait identifier des emplacements dans les données d'image/le contenu d'image où l'intégrité est mise en question. Solutions possibles:

  1) méthodes cryptographiques telles que codes d'authentification de message (MAC, *message authentication code*), signatures numériques, sommes de contrôle cryptographique ou adressage dispersé sur clés calculées;

  2) méthodes fondées sur un filigranage. La présente Recommandation | Norme internationale ne définit pas de modèle normatif pour la technique de filigranage, bien qu'elle prenne en charge les outils non normatifs utilisant cette technique;

  3) combinaison des deux types de méthode précédents.

– *Authentification de l'origine*

  Un fichier JPSEC peut prendre en charge une vérification de l'identité d'un utilisateur/correspondant qui a produit le fichier JPSEC. Cette vérification peut faire appel à des méthodes telles que les signatures numériques ou le code d'authentification de message (MAC).

– *Accès conditionnel*

  Un fichier JPSEC peut prendre en charge un mécanisme et une politique permettant d'octroyer ou d'interdire l'accès à des données d'image ou à des portions de celles-ci. Ce procédé pourrait par exemple autoriser une (pré)visualisation à basse résolution d'une image sans qu'il soit possible de visualiser une résolution supérieure.

– *Identification d'un contenu enregistré*

  Un fichier JPSEC peut être enregistré auprès d'un organisme d'enregistrement de contenu. Il peut prendre en charge une méthode de vérification de concordance entre les données d'image/le contenu d'image (que l'on revendique) et les données d'image/le contenu d'image que l'on a enregistré. Par exemple, de telles méthodes pourraient être les suivantes: lecture d'un identificateur de fichier (plaque d'immatriculation) qui a été placé à l'intérieur des métadonnées, vérification de la cohérence entre cette plaque d'immatriculation et les informations qui ont été téléchargées en exportation quand le processus d'enregistrement a été effectué. La plaque d'immatriculation pourrait contenir assez d'informations pour être en mesure de demander des renseignements auprès de l'organisme d'enregistrement de contenu où le fichier a été enregistré et de vérifier que ce fichier correspondent à l'identificateur.

– *Flux direct à échelonnement et transcodage sécurisés*

  Un fichier JPSEC ou une séquence de paquets JPSEC peut prendre en charge des méthodes telles que le même nœud (ou un nœud différent) puisse exécuter la transmission en flux direct et le transcodage sans nécessiter de déchiffrement ni de déprotection du contenu. Un exemple est le cas où un contenu JPEG 2000 protégé est transmis en flux direct à un nœud ou à un serveur intermédiaire à mi-réseau, qui à son tour transcode le contenu JPEG 2000 protégé d'une façon qui préserve la sécurité de bout en bout.

5.3 Commentaires sur la conception et l'implémentation de systèmes JPSEC (sécurisés)

La présente Recommandation | Norme internationale prend en charge un riche et flexible ensemble de services de sécurité. Par exemple, les primitives de chiffrement peuvent être appliquées de différentes façons afin d'atteindre différents objectifs, allant du chiffrement de la totalité du flux à codage JPEG 2000 au chiffrement sélectif d'une petite portion seulement du flux codé. Il importe toutefois de souligner que des précautions particulières doivent être prises lors de l'implémentation d'un quelconque système de sécurité, même fondé sur la syntaxe JPSEC.

Il est fortement recommandé que les concepteurs de tous les systèmes de sécurité examinent de près les directives recommandées au sujet des primitives de sécurité qui peuvent être employées. Pour la plupart des primitives de sécurité signalées au moyen de la syntaxe JPSEC, les normes ISO/CEI associées offrent d'importantes indications sur leur usage correct. Par exemple, pour un chiffrement utilisant un algorithme par blocs et un mode associé de chiffrement par blocs (Tableau 29), des directives sur le choix et le fonctionnement du mode de chiffrement par blocs sont données dans l'ISO/CEI 10116.

Par ailleurs, dans de nombreuses applications de sécurité, l'authentification est le plus important service de sécurité. Même quand la confidentialité est le service de sécurité recherché, celui-ci devrait être augmenté par une authentification afin d'empêcher diverses formes d'attaques. Spécifiquement, même dans de nombreuses applications d'imagerie où l'objectif premier est la confidentialité, il est recommandé que l'authentification soit également employée.

La gestion des clés est hors du domaine d'application de la syntaxe JPSEC; cependant sa criticité doit encore être soulignée. Dans tout système cryptographique, la gestion des clés cryptographiques qui commandent les opérations est d'une importance cruciale. Si ces clés sont compromises, alors la sécurité de l'ensemble du système est compromise au point que cette compromission puisse ne pas être détectée. Il est donc impératif que les clés soient produites, distribuées, mémorisées et détruites à un niveau de sécurité qui soit au moins égal à celui des données qu'elles sont censées protéger. Par ailleurs, comme la probabilité qu'une clé soit compromise augmente avec le temps, il est également impératif que les clés ne soient utilisées que pendant une durée fixe de leur vie. Pour plus d'informations sur l'utilisation et la gestion des clés cryptographiques, voir l'ISO/CEI 11770.

Comme avec tous les systèmes de sécurité, l'utilisation d'opérations cryptographiques doit être complètement opaque à l'utilisateur. C'est-à-dire que celui-ci ne devrait pas être en mesure de découvrir de quelconques informations sur les opérations cryptographiques, sauf pour la sortie. Par exemple, l'utilisateur ne devrait pas être en mesure d'accéder à des informations concernant la raison pour laquelle une opération cryptographique n'a pas réussi à produire une sortie. De même, un utilisateur ne devrait pas être en mesure de trouver de quelconques informations complémentaires même s'il recourt au mesurage des "canaux latéraux" comme l'analyse du rythme et/ou de la puissance. En bref, l'utilisateur ne devrait pas être en mesure de remarquer une quelconque différence dans l'une quelconque des sorties applicatives,

quelle que soit l'application qu'il est actuellement en train d'exécuter car, si tel n'est pas le cas, la fuite d'informations résultante pourra éventuellement compromettre la sécurité du système.

En résumé, il est fortement recommandé que le concepteur d'un système de sécurité, fondé ou non sur la syntaxe JPSEC, prête une attention particulière aux détails de conception de ce système afin de garantir sa sécurisation.

5.4 Segment verrouillé en octets (BAS)

5.4.1 Segment verrouillé en octets

Afin d'offrir une signalisation extensible des classes et des modes, la présente Recommandation | Norme internationale utilise une structure de données à longueur variable, appelée *segment verrouillé en octets* (BAS, *byte aligned segment*). Les champs paramétriques dont le nombre est extensible sont représentés avec la structure de segment verrouillé en octets de champ (FBAS, *field byte aligned segment*). Les valeurs paramétriques ayant une grande étendue sont représentées sous forme extensible, au moyen de la structure de segment verrouillé en octets d'étendue (RBAS, *range byte aligned segment*).

Comme décrit dans la Figure 2, le segment BAS se compose d'une séquence d'un ou de plusieurs octets de segments BAS. Le bit de plus fort poids (MSB, *most significant bit*) de chaque octet de segment BAS indique l'existence d'un octet de segment BAS subséquent. Spécifiquement, si MSB = 1, alors un octet subséquent de segment BAS existe, alors que si MSB = 0, alors un octet subséquent de segment BAS n'existe pas et la structure à segments BAS est terminée. Les bits de plus faible poids qui restent dans chaque octet de segment BAS sont concaténés de façon à former une liste de bits qui sont utilisés de différentes façons pour différents paramètres à segments BAS: ils sont souvent utilisés dans le cadre d'une liste de paramètres ayant un certain nombre d'éléments et chaque bit de segment BAS est réglé à 1 ou 0 afin de signaler par un fanion des informations sur son élément correspondant. Cette structure flexible a été choisie en raison de son extensibilité en vue de futures évolutions de la norme, car elle permet de signaler de nouveaux paramètres de façon extensible.

Figure 2 – Structure d'un segment verrouillé en octets (BAS)

5.4.2 Segment BAS de champ (FBAS)

Un segment BAS de champ (FBAS) est un type de segment BAS où les bits restants des octets de segments BAS servent à mettre les champs à 1 ou à 0. Un exemple d'utilisation de segment FBAS est la classe de description de la zone d'influence (DCzoi), où l'on peut spécifier de multiples descriptions d'image telles que l'indice de pavé, le niveau de résolution et la composante chromatique. Si l'on fait ainsi, l'on signalera, en mettant le fanion à 1, les trois bits de segment BAS correspondant à: pavé, résolution et couleur.

Par exemple, si l'on souhaite représenter un segment BAS de champ avec 9 champs, de f1 à f9, alors l'on aura besoin d'utiliser au plus deux octets de segments BAS. Si les deux octets ont été "a" et "b" et si le bit de plus fort poids de chaque octet a été a0 et b0, alors le segment FBAS aura l'allure suivante:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

a0 et b0 sont les bits indicateurs. Les champs f1 à f7 sont représentés par les bits a1 à a7, le champ f8 est représenté par le bit b1 et le champ f9 est représenté par le bit b2. Les bits b3 à b7 restants sont réservés et réglés à 0.

a0 f1 f2 f3 f4 f5 f6 f7 | b0 f8 f9 0 0 0 0 0

Quand il est utilisé dans un flux JPSEC, le segment FBAS figurant dans cet exemple peut être représenté par un ou deux octets, selon les valeurs réelles du champ. Cela s'explique par le fait que la valeur par défaut des champs est 0. Donc, si les champs f8 et f9 ne sont pas activés (c'est-à-dire si leur valeur est 0), alors le second octet du segment BAS n'est pas requis et a0 est réglé à 0. D'autre part, si le champ 8 ou le champ 9 est activé, alors deux octets sont requis. Dans ce cas, a0 est réglé à 1 et b0 est réglé à 0.

Noter que les bits du champ sont "alignés à gauche". Cela permet d'ajouter plus de champs au cours du temps, d'une façon compatible.

5.4.3 Segment BAS d'étendue (RBAS)

Le segment BAS d'étendue (RBAS) sert à élargir l'étendue ou le nombre de bits servant à représenter une valeur. Il y a deux types de segment RBAS: RBAS-8 et RBAS-16.

Le segment RBAS-8 contient un ou plusieurs octets de segment RBAS qui contiennent les bits de la valeur. Comme dans le segment FBAS, le premier bit de chaque octet indique si un autre octet RBAS suit.

Contrairement au segment FBAS, le segment RBAS est "aligné à droite". Donc, si une valeur a 9 bits significatifs de v1 à v9, où v1 est le bit de plus fort poids, alors cette valeur serait représentée par deux octets de segment BAS:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

comme suit:

1 0 0 0 0 0 v1 v2 | 0 v3 v4 v5 v6 v7 v8 v9

Si la valeur était assez petite pour que les bits v1 et v2 aient été zéro, alors la représentation par deux octets ci-dessus pourra être utilisée avec v1 et v2 réglés à zéro, ou un segment RBAS d'un seul octet pourra être utilisé comme représenté ci-dessous:

0 v3 v4 v5 v6 v7 v8 v9

Le segment RBAS-16 peut servir à représenter des valeurs qui comptent normalement plus de 7 mais moins de 15 bits. Dans ce cas, le premier fragment de segment RBAS aura deux octets dans lesquels: le premier bit sera l'indicateur; les 15 bits suivants seront les bits de valeur; puis les octets restants auront étendu un seul octet à la fois au moyen de la structure normale de segment BAS où le premier bit de chaque octet est l'indicateur d'octets suivants de segment BAS.

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7 | c0 c1 c2 c3 c4 c5 c6 c7

Si une valeur paramétrique avait 22 bits, alors elle pourra être représentée par la structure à trois octets de segment RBAS-16 représentée ci-dessous, où a0 et c0 sont des bits indicateurs spécifiant si un octet de segment BAS suit. Tous les octets restants de segment BAS sont des segments BAS traditionnels à un seul octet.

a0 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | c0 v16 v17 v18 v19 v20 v21 v22

Donc, les bits indicateurs seront réglés comme suit:

1 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | 0 v16 v17 v18 v19 v20 v21 v22

Pour les deux segments RBAS-8 et RBAS-16, les bits de valeur sont également "alignés à droite".

Noter que, lors de la rédaction de créateurs et de consommateurs JPSEC, il est important de veiller aux représentations gros-boutistes/petit-boutistes.

5.5 Marqueur de sécurité principal (SEC)

5.5.1 Segments marqueurs de sécurité

Dans le présent paragraphe, l'on présente une syntaxe simple et flexible, quoique puissante, pour la signalisation JPSEC. Les segments marqueurs SEC sont définis à cette fin et sont situés dans l'en-tête principal. La syntaxe de segment marqueur SEC permet de décrire toutes les informations requises pour sécuriser des images JPEG 2000. A cette fin, cette syntaxe fait référence à des outils JPSEC normatifs qui sont spécifiés par les modèles décrits dans le § 5.8 ou par des outils JPSEC non normatifs qui peuvent avoir été enregistrés au préalable auprès de l'organisme d'enregistrement JPSEC ou avoir été définis secrètement. La syntaxe énonce également des dispositions pour le traitement des paramètres associés à ces outils.

Un flux à codage JPSEC peut être protégé au moyen d'un ou de plusieurs outils JPSEC, qui sont normatifs ou non normatifs. Les paramètres de ces outils sont signalés dans un ou plusieurs segments marqueurs SEC situés dans l'en-tête principal du flux codé après le segment marqueur SIZ. Quand de multiples segments marqueurs SEC sont utilisés, ils sont concaténés et doivent apparaître consécutivement dans l'en-tête principal. Dans la plupart des cas, tous les paramètres JPSEC peuvent être signalés dans un seul segment marqueur SEC. Cependant, dans certains cas, la longueur