NORME INTERNATIONALE

ISO
8732

Première édition
1988-11-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION
МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

Banque — Gestion de clés

Banking — Key management (wholesale)

Numéro de référence
ISO 8732 : 1988 (F)

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour approbation, avant leur acceptation comme Normes internationales par le Conseil de l'ISO. Les Normes internationales sont approuvées conformément aux procédures de l'ISO qui requièrent l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 8732 a été élaborée par le comité technique ISO/TC 68, *Banque et services financiers liés aux opérations bancaires.*

L'attention des utilisateurs est attirée sur le fait que toutes les Normes internationales sont de temps en temps soumises à révision et que toute référence faite à une autre Norme internationale dans le présent document implique qu'il s'agit, sauf indication contraire, de la dernière édition.

Imprimé en Suisse

Sommaire

Figures

Tableaux

Introduction

La présente Norme internationale décrit des procédures destinées à sécuriser la gestion des clés secrètes utilisées pour protéger des messages bancaires liés à l'activité d'entreprise, tels que des messages entre banques, ou entre une banque et une société cliente, ou entre une banque et une administration.

La gestion de clé consiste à fournir aux deux entités des clés de chiffrement et des motifs d'initialisation (éléments de mise à la clé) qui resteront soumis à des procédures de traitement protégé jusqu'à leur destruction. La sécurité des données chiffrées au moyen de ces éléments de mise à la clé dépend des mesures prises contre la divulgation, la modification, la substitution, l'insertion ou l'effacement non autorisés des clés et des motifs d'initialisation (IVs). Si ces éléments sont compromis, la sécurité des données concernées ne peut plus être garantie. La gestion de clé vise donc la création, la distribution, le stockage, la mémorisation, la surveillance, la destruction et la sauvegarde des éléments de mise à la clé. La formalisation de ces procédures doit enfin permettre de retracer le déroulement des opérations à des fins d'audit.

La distribution automatique des clés consiste en la transmission électronique des clés (et, quand celà est nécessaire des, IVs) par l'utilisation d'un moyen de communication. La distribution automatique de clés fait appel à deux types de clés:

(1) Clés de chiffrement de clés : elles servent à chiffrer ou déchiffrer d'autres clés.

(2) Clés de données : elles servent à chiffrer ou déchiffrer les motifs d'initialisation (IVs), à authentifier les messages de service de chiffrement, et à chiffrer/déchiffrer ou authentifier les données.

Les installations de gestion de clé peuvent être conçues pour renouveler automatiquement les clés de chiffrement de clés et les clés de données. Dans ce cas, l'intervention manuelle est extrêmement faible. Les clés de chiffrement de clés ont généralement une période de validité supérieure à celle des clés de données.

Le degré de sécurité à atteindre doit être lié à un grand nombre de paramètres tels que la sensibilité des données traitées, leur probabilité d'interception, la facilité de mise en oeuvre du mécanisme de chiffrement envisagé et le coût lié à la mise en oeuvre et à la rupture d'un mécanisme particulier de sécurité. Il est donc nécessaire que chaque couple d'interlocuteurs s'entende sur la portée et les détails des techniques de sécurité et de gestion de clés. Une sécurité absolue n'est pas réalisable pratiquement; la gestion de clés doit viser non seulement à réduire la probabilité d'effraction, mais aussi à offrir une forte probabilité de détection de tout accès ou changement illégal des éléments de mise à la clé, toujours possibles malgré toutes les mesures préventives. Ceci s'applique à toutes les étapes de la création, de l'échange et de l'exploitation des éléments de mise à la clé, y compris aux opérations effectuées à l'intérieur des matériels de chiffrement et de transmission des clés et des motifs d'initialisation entre couples d'interlocuteurs ou centres de chiffrement. Même si la présente Norme internationale spécifie chaque fois que possible des exigences en termes absolus, il demeure que dans certains cas, une certaine part de subjectivité ne peut être techniquement écartée. La définition de la fréquence des changements de clé échappe ainsi au cadre de la présente Norme et dépendra de la part de risque liée aux paramètres énoncés ci-dessus.

La présente Norme internationale comprend trois sections:

Un: Généralités
Deux: Distribution manuelle des éléments de mise à la clé
Trois: Distribution automatique des éléments de mise à la clé

Les derniers détails des procédures de gestion de clé doivent faire l'objet d'un accord entre les couples d'interlocuteurs concernés et demeurent donc sous leur responsabilité. Parmi ces détails, retenons l'identité et les attributions des différents interlocuteurs. La présente Norme ne traite pas de la définition des responsabilités individuelles, aspect qui est spécifique de chaque mise en oeuvre de gestion de clés.

L'annexe A fournit un exemple de mise en oeuvre des exigences prévues au titre de la distribution manuelle des éléments de mise à la clé.

Page blanche

Banque — Gestion de clés

Section 1: Généralités

1 Objet et domaine d'application

La présente Norme internationale spécifie des méthodes de gestion d'éléments de mise à la clé destinés au chiffrement, au déchiffrement et à l'authentification des messages échangés lors des transactions financières liées à l'activité d'entreprise. Elle spécifie des exigences

i) quant au contrôle des éléments de mise à la clé pendant leur période de validité, pour empêcher la divulgation, la modification, la substitution et la réutilisation non autorisées;

ii) quant à la distribution manuelle ou automatique des éléments de mise à la clé, afin de permettre l'interopérabilité entre matériels ou dispositifs de chiffrement utilisant le même algorithme;

iii) visant l'intégrité des éléments de mise à la clé pendant toutes les phases de la période de validité : création, distribution, stockage, saisie, utilisation, archivage et destruction;

iv) visant à récupérer les informations en cas d'échec du processus de gestion de clés ou si l'intégrité des éléments de mise à la clé est mise en cause.

La présente Norme permet également de retracer au cours d'un audit ultérieur tous les éléments de mise à la clé utilisés.

La présente Norme internationale est conçue pour l'utilisation d'algorithmes symétriques dans la distribution des clés, l'expéditeur et le destinataire utilisant la même clé. Elle s'applique à des messages formatés et transmis à partir de jeux de caractères codés. Il est prévu d'aborder ultérieurement l'utilisation d'algorithmes asymétriques dans la distribution des clés.

La présente Norme ne permet pas de distinguer, d'un point de vue cryptographique, deux entités physiques partageant la même clé.

Les procédures spécifiées ici sont destinées aux institutions financières et à leurs clients (sociétés ou administration) et dans toutes autres relations où l'échange d'informations nécessite la confidentialité, la protection et l'authentification.

2 Références

ISO 646, *Traitement de l'information — Jeu ISO de caractères codés à 7 éléments pour l'échange d'information.*

ISO 7982-1, *Télécommunications bancaires — Messages de transfert des fonds — Partie 1: Vocabulaire et éléments de données.*

ISO 8372, *Traitement de l'information — Mode opératoire d'un algorithme de chiffrement par bloc de 64 bits.*

ISO 8730, *Opérations bancaires — Spécifications liées à la normalisation de l'authentification des messages.*

ISO 8731, *Banque — Algorithmes approuvés pour l'authentification de messages.*

ANSI X3.92, *Data Encryption Algorithm.*

3 Définitions

Dans le cadre de la présente Norme internationale, les définitions suivantes sont applicables:

3.1 trace d'audit: Voir *trace d'audit de sécurité*.

3.2 authentification: Méthode employée par l'expéditeur et le destinataire pour s'assurer de *l'intégrité des données*, et fournir un moyen *d'authentifier leur origine*.

3.3 biais: Phénomène lié à la création de nombre aléatoires ou pseudo-aléatoires faisant que certains nombres sortent plus souvent que d'autres.

3.4 cryptogramme: Informations chiffrées.

3.5 code: Façon symbolique de représenter des données permettant de faciliter un traitement automatisé.

3.6 couple d'interlocuteurs: Deux *entités logiques* d'accord pour échanger des données.

NOTE — Une entité et un centre de distribution ou de traduction de clés échangeant des messages de service de chiffrement ne constituent pas un couple d'interlocuteurs.

3.7 Temps Universel Coordonné (TUC): L'échelle de temps conservée au Bureau international de l'Heure, qui sert de base à une distribution co-ordonnée des fréquences normalisées et des signaux temporels.

NOTE — Peut aussi être appelé Heure de Greenwich (GMT).

3.8 compteur: Compteur incrémentiel utilisé par deux entités pour contrôler les attributions successives de clés à partir d'une *clé particulière de chiffrement de clés*.

3.9 équipement de chiffrement: Équipement à l'intérieur duquel ont lieu les fonctions de chiffrement (*chiffrement, authentification, création de clés*).

3.10 clé de chiffrement; clé: Paramètre complémentaire d'un algorithme servant à la *validation, l'authentification, le chiffrement* ou le *déchiffrement.*

3.11 chiffre: Discipline que englobe tous principes, moyens et méthodes destinés à la transformation de données afin de cacher leur contenu, d'empêcher leur modification et leur utilisation frauduleuses.

NOTE — Le chiffre définit les méthodes de *chiffrement* et *déchiffrement*. L'attaque d'un principe, de moyens ou de méthodes cryptographiques est applelée cryptanalyse.

3.12 période de validité: Période prédéfinie durant laquelle une *clé donnée* peut être utilisée ou durant laquelle les *clés d'un système* donné restent valides.

3.13 intégrité des données: Capacité qu'ont des données de ne pas pouvoir être altérées ou détruites d'une manière frauduleuse.

3.14 clé de donnée: *Clé* utilisée pour le *chiffrement*, le *déchiffrement* ou l'*authentification* des données.

3.15 authentification de l'origine des données: Constatation que l'expéditeur des données reçues est bien celui qu'il prétend être.

3.16 déchiffrement: Transformation inverse d'un *chiffrement* réversible correspondant.

3.17 double contrôle: Intervention de deux entités distinctes ou plus (généralement des personnes) opérant de concert pour protéger des fonctions ou des informations sensibles, aucun individu isolé ne pouvant accéder aux éléments ni les utiliser, par exemple une *clé de chiffrement*.

3.18 chiffrement: Transformation chiffrée de données (voir *chiffre*) aboutissant à un *cryptogramme*.

3.19 ou-exclusif: voir *addition modulo-2*.

3.20 étiquette de champ: Chaîne de caractères unique figurant dans les messages formatés pour identifier la signification et l'emplacement du champ de données associé.

3.21 message financier: Communication comportant des informations à caractère financier.

3.22 chiffre hexadécimal: Caractère unique choisi dans l'intervalle 0-9, A-F (majuscules) représentant une configuration de 4 bits.

3.23 motif d'initialisation (IV): Nombre servant de point de départ au *chiffrement* d'une séquence de données pour accroître la sécurité en introduisant une variation cryptographique supplémentaire et pour synchroniser l'*équipement de chiffrement*.

3.24 interopérabilité: Aptitude à échanger des *clés*, manuellement ou automatiquement, avec une autre entité.

3.25 clé: voir *clé de chiffrement*.

3.26 élément de clé: Paramètre parmi deux ou plus qui a le format d'une *clé de chiffrement* et qui est ajouté *modulo-2* à un ou plusieurs paramètres semblables pour former une *clé de chiffrement*.

3.27 centre de distribution de clés: Lieu où sont générées les *clés de chiffrement* et d'où elles sont expédiées.

3.28 clé de chiffrement de clé: *Clé* servant au *chiffrement* et au *déchiffrement* de *clés*.

3.29 générateur de clé: Dispositif de création de *clé de chiffrement* et de *vecteur d'initialisation* si besoin est.

3.30 chargeur de clé: Unité électronique autonome capable de stocker au moins une *clé et de la charger* à la demande dans *l'équipement de chiffrement*.

3.31 dispositif de gestion de clé: Enceinte protégée (par exemple: salle ou *appareil*) et contenu de celle-ci, où résident les éléments de chiffrement.

3.32 décalage: Résultat de l'addition d'un *compteur* à une *clé* en utilisant l'*addition modulo-2*.

3.33 centre de traduction de clés: Lieu où sont transformées les *clés de chiffrement* et d'où elles sont expédiées.

3.34 élément de mise à la clé: Données (exemple: clés et IV) nécessaires pour établir et entretenir un *contexte de chiffrement*.

3.35 contexte de chiffrement: Conditions existant entre un *couple d'interlocuteurs* qui partagent, pendant cet intervalle, au moins une *clé de chiffrement* ou une *clé de chiffrement de clé*.

3.36 entité logique: Une ou plusieurs entités physiques formant l'un des membres d'un *couple d'interlocuteurs*.

3.37 code d'authentification de message (MAC): *Code* figurant dans un message entre l'expéditeur et le destinataire pour en valider l'origine ainsi que tout ou partie du texte du message. Le *code* est le résultat d'une méthode de calcul agréée.

3.38 addition modulo-2; ou-exclusif: Addition binaire sans retenue donnant les valeurs suivantes:

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

3.39 notarisation: Méthode permettant de modifier une *clé de chiffrement de clé* dans le but d'authentifier l'identité de *l'expéditeur* et du *destinataire* final.

3.40 clé de notarisation: *Clé* utilisée pour la *notarisation*.

3.41 sceau de notarisation: Valeur créée à partir des identités des *entités logiques* d'un *couple d'interlocuteurs*, et utilisée pour créer une (ou deux) *clé(s) de notarisation*.

3.42 expéditeur: Entité logique responsable de la création d'un message de service de chiffrement.

3.43 texte clair: Données non chiffrées.

3.44 destinataire: Entité logique responsable de la réception d'un message de service de chiffrement.

3.45 audit de sécurité: Étude et examen indépendants des enregistrements et des activités du système, dans le but de mesurer l'adéquation des contrôles du système, de vérifier la conformité avec la politique en vigueur et les procédures opérationnelles et de faire des recommandations pour tout changement défini dans les contrôles, la politique suivie et les procédures.

3.46 trace d'audit de sécurité: Données rassemblées et prêtes à être fournies lors d'un *audit de sécurité*.

3.47 période de validité des données: Période durant laquelle des données chiffrées ou protégées sont valides.

3.48 connaissance répartie: Contexte dans lequel au moins deux entités se partagent en les gardant secrets les éléments d'une clé unique qui, pris isolément, ne permettent pas de déduire la *clé de chiffrement* résultant de leur combinaison.

3.49 validation: Vérification de l'*intégrité* d'un message ou d'éléments choisis de celui-ci.

3.50 abrogation: Méthode permettant l'effacement ou la réécriture de données mémorisées par un procédé électronique.

4 Abréviations

Les abréviations suivantes sont utilisées dans la présente Norme internationale:

La notation employée aux chapitres 12 à 15 est décrite à l'annexe B.

Abréviation	Signification	Description (voir également le tableau 2)
CKD	Centre de distribution de clés	Installation permettant la création et la restitution de clés en vue de leur expédition.
CKT	Centre de traduction de clés	Installation permettant la transformation et la restitution de clés en vue de leur expédition.
CSM	Message de service de chiffrement	Message destiné au transport de clés ou d'informations connexes servant à maintenir un contexte de chiffrement.
CTA	Comptage A	Compteur utilisé entre un CKD ou un CKT et l'entité «A».
CTB	Comptage B	Compteur utilisé entre un CKD ou un CKT et l'entitié «B».
CTP	Comptage P	Compteur utilisé dans un contexte de chiffrement en mode point à point
CTR	Comptage R	Valeur du compteur réputé erroné.
DEA	Data Encryption Algorithm	—
DSM	Message de service de fin de connexion	Type de message servant à invalider une ou plusieurs clés ou à mettre fin à un contexte de chiffrement.
ECB	Répertoire électronique	Un des modes opératoires d'un algorithme de chiffrement.
EDC	Code de détection d'erreur	Code d'un message de service de chiffrement servant à prouver l'intégrité des données d'un message.

Abréviation	Signification	Description
EDK	Date d'entrée en vigueur d'une clé	Date et heure du temps universel auxquelles la clé de données est mise en service.
ERF	Champ d'erreur	Identification des conditions d'erreur détectées au sein d'un message de service de chiffrement précédent.
ERS	Message de service de récupération d'erreur	Type de message servant à récupérer les erreurs de comptage ou autres en mode à centre de distribution ou de traduction de clés.
ESM	Message de service d'erreur	Type de message servant à donner un accusé de réception négatif d'un message de service de chiffrement autre qu'un ESM et à indiquer au destinataire des données lui permettant de reprendre les opérations.
IDA	Identifiant de clé d'authentification	Identifie la clé servant à authentifier un message de service de libération de connexion. La clé identifiée cesse d'être valide.
IDC	Identifiant de centre de distribution ou de traduction de clés	—
IDD	Identifiant de la clé à abandonner	—
IDK1	Identifiant de clé (sous-champ)	Identifiant de la clé transmise dans un message de service de chiffrement.
IDK2	Identificateur de clé de chiffrement de clé (sous-champ)	Identifiant (nom) de la clé (simple ou double) de chiffrement de clé servant à chiffrer la clé transmise dans un message de service de chiffrement.
IDU	Identité du destinataire final	Identité du destinataire final prévu à l'émission d'un message de service de chiffrement en mode à centre de distribution ou de traduction de clé.
IV	Motif d'initialisation	—
KD	Clé de données	Clé servant à chiffrer/déchiffrer ou authentifier des données.
KDU	Clé de données notarisée	Clé de données chiffrée d'après une clé double notarisée.
KDX	Clé de données fixe	Clé de données de valeur fixe utilisée dans le calcul d'un code de détection d'erreur.
KK	Clé de chiffrement de clés	Clé servant à chiffrer et déchiffrer des clés.
*KK[1)]	Clé double de chiffrement de clés	Ensemble de deux clés servant à chiffrer et déchiffrer des clés.
KKM	Clé principale de chiffrement de clés	Clé de chiffrement de clé de niveau supérieur dans une architecture multicouche de gestion de clés.
KKU	Clé de chiffrement de clés notarisée	Clé de chiffrement de clés chiffrée d'après une clé notarisée.
*KKU[1)]	Clé double de chiffrement de clés notarisées	Clé double de chiffrement de clés chiffrée d'après une clés double notarisée.
KN	Clé notarisée	Une clé servant à la notarisation.
KSM	Message de service de clé	Type de message servant à échanger des clés entre couple d'interlocuteurs.
MAC	Code d'authentification de message	—
MCL	Type de message	Étiquette du champ définissant le type de message de service de chiffrement.
NOS	Indicateur de notarisation	Étiquette dont la présence indique qu'une procédure de notarisation a eu lieu
NS	Sceau de notarisation	Valeur servant à la notarisation.

1) L'astérisque * indique que l'on traite une clé double. Lorsque l'utilisation d'une clé double est une option, l'astérisque figure entre parenthèses dans le texte principal.

Abréviation	Signification	Description
ORG	Expéditeur	Expéditeur d'un CSM.
P	Parité de clé (sous-champ)	Indique que la clé, avant son chiffrement, est de parité impaire.
RCV	Destinataire	Destinataire d'un CSM.
RFS	Message de demande de service	Sert à demander la traduction de clés à un centre de traduction de clés avant retransmission à une autre entité.
RSI	Message de service de demande d'établissement	Sert à demander des clés à une autre entité.
RSM	Message de service en réponse	Permet d'accuser réception de façon authentifiée.
RTR	Message de réponse au demandeur	Utilisé pour envoyer des clés depuis un centre de distribution ou de traduction de clés.
SVR	Demande de service	Spécifie le type de service demandé.

5 Dispositif de gestion de clés

5.1 Généralités

Un dispositif de gestion de clés doit offrir les moyens de contrôle d'accès qui protègent son contenu de divulgation, modification, substitution, répétition, insertion ou suppression non autorisés.

NOTE — Dans ce but, des mesures doivent être prises soit pour empêcher l'accès soit pour veiller à ce que les tentatives d'accès aient toutes les chances d'être détectées puis signalées.

5.2 Contenu d'un dispositif de gestion de clés

Tout le matériel de chiffrement, y compris le matériel d'élaboration de clés, doit être situé au sein d'un dispositif de gestion de clés.

NOTE — Le matériel de chiffrement peut jouer le rôle de dispositif de gestion de clés et offrir ainsi toutes les fonctions requises.

6 Spécifications de l'équipement de chiffrement

6.1 Élaboration des clés et des motifs d'initialisation (IV)[1)]

6.1.1 Généralités

Les procédures d'élaboration de clés et de motifs d'initialisation doivent être placées sous une double responsabilité.

L'élaboration des clés et des motifs d'initialisation doit s'effectuer selon un processus garantissant que toutes les clés et les motifs d'initialisation soient obtenus de façon aléatoire ou pseudo-aléatoire. Le processus de création doit être conçu de sorte qu'aucun avantage ne réside dans le fait de s'attaquer au processus d'élaboration de clé plutôt qu'au processus de chiffrement.

Le résultat du processus d'élaboration de clé doit être contrôlé automatiquement afin de détecter les erreurs de création (par exemple la sortie répétée d'une même clé). Le fonctionnement du générateur de clé doit s'interrompre immédiatement si une défaillance quelconque est constatée.

Le matériel de chiffrement ne doit pas fournir les clés en clair, même en cas de défaillance, si ce n'est lors de la création même de la clé.

Il doit être possible de mettre à zéro manuellement les clés délivrées en clair (voir annexe F).

6.1.2 Clés et motifs d'initialisation destinés à une distribution manuelle

Tous les supports entrant dans l'élaboration, la distribution et le stockage (notamment les exemplaires sur papier, les rubans etc.) doivent être protégés contre une utilisation, modification, remplacement, destruction ou exposition non autorisés. Les déchets doivent être détruits sous double contrôle. Le processus de création de clés doit avoir lieu dans un espace protégés des regards indiscrets.

Lorsque des clés ou des motifs d'initialisation sont imprimés, des moyens doivent être prévus pour empêcher qu'ils soient divulgués ou remplacés.

NOTE — Une telle protection peut notamment s'appuyer sur des registres de clés à exemplaires uniques aux pages numérotées, protégée par un conditionnement résistant aux effractions de sorte que le remplacement de page soit impossible.

En présence d'un dispositif spécial à mémoire électronique protégée, des mécanismes de sécurité doivent être intégrés au logiciel ou au matériel pour interdire l'accès non autorisé. Toute tentative d'accès illégal à la mémoire protégée doit entraîner l'effacement automatique de la clé conservée en clair, ou du moins sa mise sous forme incompréhensible. Il ne doit exister aucune possibilité d'affichage ni de contrôle ni d'extraction de la clé mémorisée sans que le dispositif à mémoire protégée électroniquement soit relié à ou introduit dans un récepteur fiable.

1) De l'anglais «Intialisation Vector».

Lorsque la distribution d'une clé s'appuie sur une connaissance répartie des informations, à des fins de sécurité, chaque élément constitutif de la clé doit être établi sur un formulaire ou un support d'enregistrement indépendant.

6.1.3 Clés et motifs d'initialisation destinés à une distribution automatique

Lorsqu'un matériel de chiffrement est employé à la création automatique de clés et de motifs d'initialisation, il doit être physiquement protégé contre:

1) la divulgation, la modification et le remplacement des clés

2) la modification ou le remplacement des IV

3) la modification ou le remplacement de l'algorithme ou du dispositif de création de clé.

6.2 Chargement des clés

6.2.1 Généralités

Le matériel de chiffrement doit permettre soit au niveau du système soit du dispositif, de charger des clés au format conforme avec la présente Norme internationale. L'accès aux commandes ou systèmes de chargement de clés doit être limité physiquement ou par programme, voire les deux à la fois.

6.2.2 Chargement manuel des clés

Il doit être possible de charger manuellement les clés ou les éléments de clé. On doit pouvoir également corriger les erreurs isolées ou re-saisir l'ensemble de la clé. Si un élément de clé est affiché en clair, il ne doit être visible que pour le personnel autorisé et doit être effacé immédiatement après le chargement.

NOTE — Le rechargement d'une clé complète peut également servir à vérifier une clé saisie auparavant.

6.2.3 Chargement automatique des clés

Lorsque les clés peuvent être chargées automatiquement, la clé ne doit pas s'afficher au cours de cette opération. Les clés conservées dans des dispositifs spéciaux tels que des supports de clés doivent être chargés sous double contrôle.

6.2.4 Contrôle de parité

Si le contrôle de parité est possible, la parité des clés ou des composants de clés en clair doit être vérifiée lors du chargement, afin d'empêcher la modification inopinée d'un élément binaire de la clé.

6.2.5 Stockage des clés en clair

Toute trace en clair de clés utilisée lors du chargement de la clé doit être abrogée une fois terminé le transfert de la clé à un autre emplacement.

6.2.6 Conservation de clés mémorisées électroniquement

Une panne de courant de faible durée ne doit pas entraîner la perte d'une clé.

6.2.7 Interférences électromagnétiques

Une protection doit exister contre la détérioration de clés par rayonnement ou conduction d'interférences électromagnétiques imputables au matériel de chiffrement ou aux chargeurs de clés.

6.2.8 Essai de fonctionnement

Immédiatement avant la saisie manuelle de clés et l'initialisation du système, on doit soumettre le matériel de chiffrement à un essai, afin de s'assurer de son bon fonctionnement. Cet essai doit porter sur toutes les fonctions de commande.

6.2.9 Erreur de manipulation ou défaillance

Un dispositif doit être fourni pour signaler une défaillance ou une manipulation incorrecte du matériel de chiffrement (voir également 6.1.1). Une procédure manuelle ou automatique doit être fournie pour signaler toutes ces erreurs ou défaillances de façon détaillée.

6.3 Contrôle de compteur

Lorsque les clés sont associées à des compteurs (voir 12.2), le matériel de chiffrement doit permettre de détecter et de signaler l'effacement, la perte ou la régression d'un compteur.

7 Éléments de mise à la clé

7.1 Transport et stockage des éléments de mise à la clé

Les éléments de mise à la clé doivent être transportés et stockés de sorte qu'ils soient protégés contre la modification ou la substitution et à empêcher la mise à découvert de clés en clair pendant la période de validité des clés ou au terme de celle-ci.

L'accès au lieu de stockage y compris les mouvements de tout élément de mise à la clé à partir de ce lieu ou vers celui-ci doivent être placés sous double contrôle. Lors de l'introduction ou de la suppression d'éléments de mise à la clé, l'accès physique doit être spécifiquement autorisé, être protégé par des moyens physiques ou logiques et faire l'objet de rapports détaillés.

7.2 Clés

7.2.1 Conservation des clés

Les clés doivent être placées sous un double contrôle à tout moment. Les clés conservées sur ordinateur doivent être chiffrées ou inaccessibles.

Il doit exister des listes de membres du personnel habilités à détenir ces clés ou à y accéder. Ces listes ne doivent pas contenir d'indication quant au contenu des clés.

7.2.2 Validité des clés

On doit normalement associer aux clés un identifiant unique ou une date d'entrée en vigueur et le couple d'interlocuteurs doit convenir de la période de validité de chaque clé.

Les clés de données peuvent être échangées dès lors qu'elles sont destinées à un usage immédiat ou ultérieur (voir 7.2.4). Aucune clé ne doit être opérationnelle tant que le destinataire n'a pas retourné un accusé de réception authentifié. Si une clé n'a pas été identifiée spécifiquement (par exemple par un numéro ou une date d'entrée en vigueur), elle doit être la seule clé de son espèce et être mise en service par le couple d'interlocuteurs dès la réception par l'expéditeur de l'accusé de réception établi par le destinataire.

Si l'on suspecte ou si l'on sait que le secret d'une clé est compromis, celle-ci doit cesser d'être valide et être retirée du service.

7.2.3 Changements de clés

Les clés doivent être changées:

a) au terme de la période de validité; ou

b) avec l'accord des deux membres du couple d'interlocuteurs; ou

c) dès que l'on sait ou que l'on suspecte que le secret d'une clé est compromis.

Tous les changements de clés doivent faire l'objet d'accusés de réception. Si les périodes de validité d'une clé existante et d'une nouvelle clé se chevauchent, une date explicite (ou une autre référence implicite de temps), à laquelle l'ancienne clé cessera d'être valide, doit être spécifiée. Pendant cette période intermédiaire, les deux clés doivent bénéficier des mêmes garanties de sécurité.

Les clés retirées du service ne doivent pas être réutilisées, sciemment ou intentionnellement, sauf pour reconstruire un couple clé/message (voir 7.2.5).

7.2.4 Clés de réserve

Lorsque des clés sont mises en réserve pour faciliter des changements de clés, prévus ou non, elles doivent bénéficier des mêmes garanties de sécurité que les clés en service.

7.2.5 Archivage des clés

Si le stockage permanent (archivage) d'une clé à l'expiration de sa période de validité ou en cas de compromission est nécessaire, ladite clé doit recevoir une identification unique ou voir sa forme ou son format modifiés de sorte qu'il ne subsiste plus d'ambiguïté quant au fait qu'elle est archivée ou hors-service. Toutes les clés archivées doivent être chiffrées à l'aide d'une clé conçue dans ce but. Il ne doit pas être possible d'utiliser des éléments de mise à la clé archivés, si ce n'est pour reconstituer un couple clé/message.

NOTE — Les procédures détaillées d'archivage de clés dépendent de l'application et ne sont pas définies dans la présente Norme internationale.

7.2.6 Sauvegarde des clés

Lors de l'échange d'une clé sous une forme imprimée, l'exemplaire original doit être conservé à des fins de sauvegarde. Lorsque les clés sont échangées par voie automatique, une copie protégée doit être conservée en archive. Toutes les copies de sauvegarde de clés en service doivent bénéficier des mêmes garanties de sécurité que les clés en service.

7.2.7 Destruction des clés (voir également l'annexe F)

Toutes les copies des clés devenues inutiles doivent être détruites sous double contrôle. Les clés imprimées doivent être détruites par incinération, déchiquetage ou réduction en pulpe ou selon tout autre méthode adaptée.

Les clés mémorisées sur des supports magnétiques doivent être abrogées, l'accès étant protégé par mot de passe ou bien ce sont les supports magnétiques eux-mêmes qui doivent être détruits à l'instar des clés imprimées.

Un compte rendu détaillé de toutes les opérations de retrait et de destruction doit être établi à des fins d'audit ultérieur.

Page blanche

Section 2: Distribution manuelle des éléments de mise à la clé

Un exemple de distribution manuelle de clés et des procédures de contrôle figure à l'annexe A.

8 Acheminement des éléments de mise à la clé à distribution manuelle

Tous les documents accompagnant des éléments de mise à la clé distribués manuellement doivent être préparés avant la création des éléments de mise à la clé. Cette documentation doit comporter:

a) Un reçu des éléments de mise à la clé devant être signé par le destinataire.

b) Des informations concernant le destinataire.

c) Des informations visant les mots de passe requis pour accéder aux éléments distribués sur supports magnétiques ou sur des dispositifs de stockage fiables (par exemple des chargeurs de clés).

d) Lorsqu'on fait appel à un messager, un reçu que celui-ci signera.

e) Des informations concernant la date d'entrée en vigueur des éléments de mise à la clé ainsi que des détails sur l'émetteur et la date d'entrée en vigueur.

Toute documentation de ce type doit être visée par des signataires autorisés.

Les éléments de mise à la clé une fois créés (voir 6.1), l'accès aux éléments de clés doit être placé sous le régime du double contrôle et de la répartition des connaissances. Chaque élément de clé doit être placé dans une enveloppe séparée cachetée de façon à révéler toute ingérence éventuelle. Chaque enveloppe doit porter la marque de son contenu et l'adresse du responsable attitré, puis être placée dans une seconde enveloppe séparée, elle aussi cachetée et adressée au destinataire. La seconde enveloppe ne doit pas fournir d'indication quant à son contenu.

NOTE — Chaque pli comporte ainsi une enveloppe extérieure contenant une seule enveloppe intérieure ne renfermant qu'un élément unique de clé.

Les différents éléments constitutifs d'une clé doivent être expédiés, accompagnés d'un reçu, en utilisant une méthode garantissant une expédition séparée, par exemple à des jours différents. Les mots de passe permettant d'accéder aux supports magnétiques ou autres dispositifs de stockage, par exemple les chargeurs de clés, doivent être expédiés séparément dudit support ou dispositif.

Lorsque les éléments de mise à la clé sont expédiés par la poste, une méthode fiable doit être employée. Lorsque l'acheminement est effectué par un messager, celui-ci doit remettre un reçu à l'expéditeur. Le messager ne doit pas avoir connaissance de la nature du contenu d'une enveloppe.

9 Réception d'éléments de mise à la clé à distribution manuelle

À la réception d'un pli contenant un élément de clé, le destinataire doit examiner l'enveloppe intérieure pour vérifier, autant que possible, que l'on n'a pas tenté d' (ou réussi à) accéder à son contenu. Si l'on soupçonne que le secret du contenu de l'enveloppe intérieure est compromis, l'expéditeur doit en être averti sur le champ. L'authenticité des signatures apposées aux documents d'accompagnement doit être contrôlée par le destinataire. L'identité des éléments de clé, par exemple le numéro d'ordre ou la date d'entrée en vigueur, doit être enregistrée. Lorsque le destinataire de l'élément de clé juge satisfaisante l'authenticité de l'élément de clé, il doit signer puis retourner le reçu correspondant (voir 7.2.2). Les clés doivent être conservées à l'abri dès leur réception. Les enveloppes intérieures, c'est-à-dire celles contenant les éléments de clé, doivent être conservées soigneusement (voir chapitre 7).