NORME INTERNATIONALE

ISO 11568-1

Première édition
1994-12-01

Banque — Gestion de clés (services aux particuliers) —

Partie 1: Introduction à la gestion de clés

Banking — Key management (retail) —

Part 1: Introduction to key management

Numéro de référence
ISO 11568-1:1994(F)

Sommaire

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse

Imprimé en Suisse

Annexes

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 vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 11568-1 a été élaborée par le comité technique ISO/TC 68 *Banque et services financiers* liés aux opérations bancaires, sous-comité SC 6, Cartes de transactions financières, supports et opérations relatifs à celles-ci.

L'ISO 11568 comprend les parties suivantes, présentées sous le titre général *Banque — Gestion de clés (services aux particuliers)*

— *Partie 1 : Introduction à la gestion de clés*

— *Partie 2 : Techniques de gestion de clés pour les algorithmes cryptographiques symétriques*

— *Partie 3 : Cycle de vie des clés pour les algorithmes cryptographiques symétriques*

— *Partie 4 : Techniques de gestion de clés pour les algorithmes cryptographiques asymétriques*

— *Partie 5 : Cycle de vie des clés pour les algorithmes cryptographiques asymétriques*

— *Partie 6 : Schémas de gestion de clés*

L'annexe A fait partie intégrante de la présente partie de l'ISO 11568. Les annexes B, C, et D sont données uniquement à titre d'information.

Introduction

L'ISO 11568 décrit des procédures pour sécuriser la gestion des clés cryptographiques destinées à protéger les messages dans un environnement de services bancaires aux particuliers, tels que les messages échangés entre un acquéreur et un accepteur de carte ou entre un acquéreur et un émetteur de carte. La gestion des clés employées dans le cadre des cartes à circuit intégré n'est pas traitée dans l'ISO 11568, mais fera l'objet d'une autre Norme internationale.

Alors que la gestion de clés dans le cadre des services bancaires aux entreprises se caractérise par l'échange de clés dans un environnement relativement bien sécurisé, la présente partie de l'ISO 11568 prescrit les besoins de gestion de clés, applicables dans des domaines ouverts qui sont les services bancaires aux particuliers tels que les autorisations de crédit et de débit aux points de vente/points de service et les transactions aux guichets automatiques de banques (GAB).

La gestion de clés est le processus par lequel des clés cryptographiques sont fournies d'une part pour que des correspondants autorisés puissent communiquer et d'autre part pour que les clés soient soumises à des procédures de sécurité jusqu'à leur destruction. La sécurité des données chiffrées dépend de mesures destinées à empêcher la divulgation de clés ainsi que toute modification, substitution, insertion ou suppression non autorisée de ces clés. La gestion de clés concerne donc l'ensemble des procédures de génération, de stockage, de distribution, d'utilisation et de destruction de ces clés. La formalisation de telles procédures fournit également les éléments permettant d'établir des traces d'audit.

La présente partie de l'ISO 11568 ne fournit pas de méthode permettant de faire la distinction entre les différents correspondants partageant des clés communes. Les détails des procédures de gestion de clés doivent faire l'objet d'un accord entre les parties impliquées dans une communication et sont donc sous la responsabilité de ces dernières. Ainsi, l'identité et les devoirs des personnes concernées doivent être définis. L'ISO 11568 n'a pas pour objet d'attribuer des responsabilités individuelles : celles-ci devront être définies pour chaque mise en œuvre de gestion de clés.

L'ISO 9564 et l'ISO 9807 définissent l'utilisation d'opérations cryptographiques lors de transactions financières effectuées par un particulier, respectivement pour le chiffrement du PIN (numéro personnel d'identification) et l'authentification des messages. L'ISO 11568 s'applique à la gestion des clés définies dans ces normes.

En outre, les procédures de gestion de clés peuvent elles-mêmes nécessiter l'introduction de clés supplémentaires, telles que les clés de chiffrement de clé, auxquelles ces procédures s'appliquent également.

Page blanche

Banque — Gestion de clés (services aux particuliers)

Partie 1 : Introduction à la gestion de clés

1 Domaine d'application

La présente partie de l'ISO 11568 prescrit les principes de gestion de clés mis en œuvre dans les systèmes cryptographiques dans le cadre des services bancaires aux particuliers. Ces services concernent l'interface entre un dispositif d'acceptation de carte (CAD) et un acquéreur d'une part, et entre un acquéreur et un émetteur de carte d'autre part. Un exemple de ce type d'environnement est illustré dans l'annexe B. Les menaces liées à l'application de la présente partie de l'ISO 11568 dans le cadre des services aux particuliers sont présentées dans l'annexe C.

Sauf spécification contraire, la présente partie de l'ISO 11568 est applicable à la fois aux clés des systèmes cryptographiques symétriques, où le donneur d'ordre et le destinataire partagent la (les) même(s) clé(s) secrète(s), et aux clés secrètes et publiques des systèmes cryptographiques asymétriques. La procédure d'approbation d'un algorithme cryptographique pour la gestion de clés est décrite dans l'annexe A.

Les algorithmes cryptographiques requièrent souvent des informations de contrôle supplémentaires, telles que les vecteurs d'initialisation et les identificateurs de clé. Ces informations sont désignées sous les termes génériques «données annexes aux clés». Bien que la présente partie de l'ISO 11568 concerne essentiellement la gestion de clés, les principes, services et techniques qui y sont décrits peuvent également s'appliquer aux éléments annexes aux clés.

La présente partie de l'ISO 11568 est destinée aux institutions financières et autres organismes fournissant des services financiers aux particuliers, pour lesquels l'échange d'informations obéit à des impératifs de confidentialité, d'intégrité ou d'authentification. Les services financiers aux particuliers incluent, sans être limités à de tels processus, les autorisations de crédit et de débit aux points de vente/points de service, les transactions réalisées aux distributeurs de billets et aux guichets automatiques, etc.

2 Référence normative

La norme suivante contient des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO 11568. Au moment de la publication, l'édition indiquée était en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO 11568 sont invitées à rechercher la possibilité d'appliquer l'édition la plus récente de la norme indiquée ci-après. Les membres de la CEI et de l'ISO possèdent le registre des normes internationales en vigueur à un moment donné.

ISO 8908:1993, *Banque et services financiers liés aux opérations bancaires — Vocabulaire et éléments de données.*

3 Définitions

Pour les besoins de la présente partie de l'ISO 11568, les définitions données dans l'ISO 8908 ainsi que les définitions suivantes s'appliquent.

3.1 algorithme cryptographique : Ensemble de règles prescrivant les procédures à appliquer pour le chiffrement et le déchiffrement des données. L'algorithme est conçu de sorte qu'il soit impossible de déterminer les paramètres de contrôle (par exemple les clés) autrement que par une recherche exhaustive.

3.2 clé cryptographique ; clé : Paramètre de contrôle d'un algorithme cryptographique ne pouvant être déduit des données en entrée et en sortie autrement que par une recherche exhaustive.

3.3 attaque par dictionnaire : Attaque par laquelle un adversaire élabore un dictionnaire de textes en clair avec leur équivalent en texte chiffré. Lorsqu'une correspondance peut être établie entre un texte chiffré intercepté et un texte chiffré répertorié dans le dictionnaire, le texte clair correspondant est fourni directement par le dictionnaire.

4 Introduction à la gestion de clés

4.1 Objet de la sécurité

Dans le cadre de services bancaires aux particuliers, les messages et les transactions contiennent des données confidentielles concernant le porteur de carte et des informations financières. L'utilisation de la cryptographie pour la protection de ces données limite les risques de pertes financières à la suite d'une fraude, préserve l'intégrité et la confidentialité des systèmes et apporte un élément de confiance dans les relations entre le fournisseur et le particulier. À cet effet, la sécurité des systèmes doit être prise en compte dans la conception globale du système. Le terme gestion de clés désigne la gestion des procédures de sécurité et des procédures système s'appliquant aux clés.

4.2 Niveau de sécurité

Le niveau de sécurité requis doit être défini en fonction de facteurs tels que la sensibilité des données concernées et leur probabilité d'interception, les possibilités pratiques de mise en œuvre du processus de chiffrement envisagé, et le coût de l'installation (et de la neutralisation) d'un dispositif de sécurité particulier. Il est donc nécessaire que les parties en communication s'entendent sur l'importance et les détails des procédures de sécurité et de gestion de clés.

4.3 Objectifs de la gestion de clés

Le premier objectif de la gestion de clés est de fournir aux utilisateurs les clés qui leur sont nécessaires pour exécuter les opérations cryptographiques prescrites et pour contrôler l'utilisation de ces clés. La gestion de clés assure également que ces clés sont protégées de manière adéquate durant leur cycle de vie. Les objectifs de sécurité de la gestion de clé sont de réduire les risques de violation de la sécurité, de limiter les conséquences d'une telle violation et d'augmenter la probabilité de détection des tentatives d'accès ou de modification de clé illicites pouvant se produire en dépit des mesures préventives. Cela concerne l'ensemble des étapes de génération, de distribution, de stockage, d'utilisation et d'archivage des clés ainsi que les processus qui interviennent dans les matériels de cryptographie et ceux liés à la communication des clés cryptographiques entre correspondants.

NOTE 1 La présente partie de l'ISO 11568 englobe tous les aspects présentés ci-dessus. La sécurité totale des systèmes inclut également la protection des communications, des systèmes de traitement de données, des équipements et des diverses installations.

5 Principes de la gestion de clés

Le respect des principes suivants est nécessaire à la protection des clés contre les menaces de violation d'un système de services bancaires aux particuliers.

a) Les clés doivent se présenter sous une forme autorisée par l'ISO 11568.

b) Personne ne doit pouvoir accéder à une quelconque clé secrète en texte clair, ni la vérifier.

c) Les systèmes doivent empêcher la divulgation de toute clé secrète ayant été utilisée pour le chiffrement de données demeurant secrètes.

d) Les systèmes doivent détecter la divulgation de toute clé secrète.

e) Les systèmes doivent prévenir ou détecter l'utilisation d'une clé secrète pour un autre but que celui prévu, ainsi que toute modification, substitution, suppression ou insertion accidentelle ou non autorisée d'une clé.

f) Les clés secrètes doivent être générées selon un processus ne permettant pas de prévoir une valeur secrète ni d'isoler des valeurs de plus grande probabilité dans l'ensemble des valeurs possibles.

g) Il convient que les systèmes permettent de détecter les tentatives de divulgation d'une clé secrète, les tentatives d'utilisation d'une clé secrète à des fins non prévues, ainsi que toute modification, substitution, suppression ou insertion non autorisée d'une clé.

h) Une clé doit être remplacée par une nouvelle clé à l'expiration d'un délai calculé en fonction du temps jugé nécessaire à la découverte de l'ancienne clé.

i) Une clé doit être remplacée par une nouvelle clé à l'expiration d'un délai jugé nécessaire à la réussite d'une attaque par référence à un dictionnaire, dirigée contre les données qu'elle a permis de chiffrer.

j) Une clé doit cesser d'être utilisée lorsque sa découverte est connue ou présumée telle.

k) La découverte d'une clé partagée par un groupe de correspondants ne doit pas permettre la découverte de clés partagées par d'autres groupes.

l) La découverte d'une clé ne doit fournir aucune information susceptible de permettre l'identification de la clé qui la remplacera.

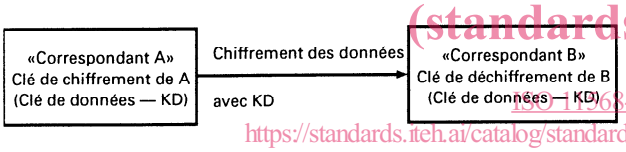
m) Une clé ne doit être chargée dans un dispositif que si celui-ci peut être considéré comme sûr et s'il n'a été soumis à aucune modification ni substitution non autorisée.

6 Systèmes cryptographiques

Un système cryptographique regroupe une opération de chiffrement et l'opération inverse, le déchiffrement. La première opération consiste à appliquer une clé de chiffrement à un texte en clair pour obtenir un texte chiffré ; la seconde opération consiste à appliquer une clé de déchiffrement à un texte chiffré afin de restituer le texte en clair. Les services bancaires aux particuliers utilisent des systèmes de ce type pour protéger les données confidentielles concernant les porteurs de cartes bancaires et les transactions financières. La donnée à protéger est chiffrée par le donneur d'ordre, puis déchiffrée par le destinataire. Il existe deux types d'algorithme cryptographiques : symétrique et asymétrique.

6.1 Algorithme cryptographique symétrique

Dans un système cryptographique symétrique, la clé de chiffrement et la clé de déchiffrement sont les mêmes ou peuvent être déduites l'une de l'autre aisément. La ou les clés doivent être tenues secrètes à la fois par le donneur d'ordre et par le destinataire. La possession de la ou des clés permet d'établir des communications sûres entre le donneur d'ordre et le destinataire. La figure 1 illustre un exemple de système cryptographique symétrique.



NOTE — La clé de chiffrement de A est identique à la clé de déchiffrement de B.

Figure 1 — Exemple de système cryptographique symétrique

Un système cryptographique symétrique en tant que tel ne permet pas de distinguer les deux extrémités du système. Néanmoins, s'il est utilisé avec les techniques de gestion de clés appropriées couplées à des dispositifs cryptographiques sûrs, il peut distinguer chaque extrémité du système et supporter des services de clé unidirectionnels. Si la même paire de clés permet la protection (par exemple chiffrement ou authentification) des données secrètes transmises dans les deux directions, on parle de clé bidirectionnelle. Lorsque la paire de clés utilisée dans une direction est différente de celle utilisée dans l'autre direction, on parle de clé unidirectionnelle.

Les principes de gestion de clés doivent être appliqués correctement pour garantir la confidentialité, l'intégrité et l'authenticité des clés secrètes.

6.2 Algorithme cryptographique asymétrique

Dans un système cryptographique asymétrique, les clés de chiffrement et de déchiffrement sont différentes, et il n'est pas possible de déduire la clé de déchiffrement à partir de la clé de chiffrement par le calcul. La clé de chiffrement d'un algorithme cryptographique asymétrique peut être rendue publique alors que la clé de déchiffrement correspondante est tenue secrète. On utilise alors les termes clé publique et clé secrète. La figure 2 illustre un système cryptographique asymétrique.

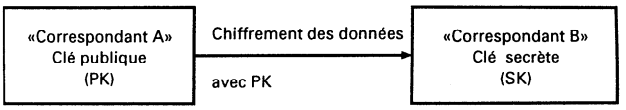


Figure 2 — Exemple de système cryptographique asymétrique

Dans un système cryptographique asymétrique, le destinataire doit détenir une clé secrète lui permettant de déchiffrer les données secrètes. Le donneur d'ordre utilise une autre clé (publique) pour chiffrer les données secrètes. Les systèmes cryptographiques asymétriques sont donc unidirectionnels par nature, c'est-à-dire qu'une paire constituée d'une clé secrète et d'une clé publique assure la protection des données transmises dans une direction seulement. La divulgation de la clé publique ne compromet pas le système. Lorsque la protection des données doit être assurée dans les deux directions, deux paires composées chacune d'une clé publique et d'une clé secrète sont requises. Les algorithmes cryptographiques asymétriques sont généralement employés pour la distribution sûre des clés initiales destinées aux systèmes cryptographiques symétriques.

Les principes de gestion de clés doivent être appliqués correctement pour garantir la confidentialité de la clé secrète, l'intégrité et l'authenticité des clés publiques et secrètes.

7 Environnements cryptographiques

Pour les systèmes cryptographiques symétriques et asymétriques, la confidentialité des clés secrètes et l'intégrité des clés publiques et secrètes lors du stockage ou de l'utilisation dépendent de la combinaison des deux facteurs suivants :

a) la sécurité du dispositif matériel chargé du processus cryptographique et du stockage des clés et autres données secrètes (voir 7.1) ; et

b) la sécurité de l'environnement cryptographique et des points de stockage des clés et autres données secrètes (voir 7.2).

La sécurité absolue ne peut pas être obtenue en pratique. En conséquence, il convient que les procédures de gestion de clés comportent des mesures préventives pour réduire les occasions de porter atteinte à la sécurité et pour augmenter les probabilités de détecter tout accès illicite aux données secrètes ou confidentielles, si ces mesures s'avéraient inefficaces.

7.1 Dispositif cryptographique sûr

Un dispositif cryptographique sûr est un dispositif qui assure un stockage sûr des informations secrètes, telles que les clés, et qui fournit des services de sécurité basés sur ces informations secrètes. Les caractéristiques et la gestion de tels dispositifs seront traitées dans une autre Norme internationale.

7.2 Environnement physiquement sûr

Un environnement physiquement sûr est doté d'un dispositif de contrôle d'accès ou d'autres systèmes conçus pour empêcher les accès non autorisés pouvant permettre la découverte de tout ou partie d'une clé ou de toute autre donnée secrète se trouvant dans cet environnement. Il peut s'agir, par exemple, d'un local sûr ou conçu spécialement et bénéficiant d'un contrôle permanent des accès, d'une protection physique et d'un système de surveillance.

Un environnement physiquement sûr doit le rester jusqu'à ce que toutes les clés et autres données secrètes, ainsi que toutes les informations récupérables découlant de ces données aient été supprimées de l'environnement ou détruites.

7.3 Réflexions sur la sécurité des clés secrètes

Les clés secrètes en clair ne doivent être conservées qu'à l'intérieur d'un «dispositif cryptographique sûr» ou dans un «environnement physiquement sûr».

Lorsque plusieurs correspondants risquent d'être affectés par la découverte de clés secrètes en clair, celles-ci doivent être conservées à l'intérieur d'un dispositif cryptographique sûr. Lorsqu'un seul correspondant risque d'être affecté, les clés doivent être conservées soit à l'intérieur d'un dispositif cryptographique sûr, soit dans un environnement physiquement sûr géré pour son compte ou par lui-même.

7.4 Réflexions sur la sécurité des clés publiques

En principe, il est inutile de protéger les clés publiques contre le risque de divulgation. Il faut néanmoins assurer une protection physique ou logique des clés publiques afin d'en empêcher la substitution illicite. Par ailleurs, il est nécessaire d'assurer la protection des données secrètes devant être chiffrées au moyen d'une clé publique.

7.5 Protection contre la contrefaçon de dispositifs

Une protection doit être introduite pour rendre impossible le remplacement du dispositif d'origine par un dispositif contrefait doté, outre ses fonctions légitimes, de fonctions non autorisées permettant de découvrir des données secrètes avant leur chiffrement.

8 Techniques de gestion de clés pour les algorithmes cryptographiques symétriques

Les services de gestion de clés sont utilisés dans les systèmes cryptographiques symétriques en application des principes exposés à l'article 5. Ces services sont brièvement décrits ci-après. (Les techniques employées pour la mise en œuvre de ces services sont décrites dans l'ISO 11568-2).

8.1 Séparation

La séparation des clés garantit que le processus cryptographique ne peut fonctionner qu'avec les types de clés spécifiquement associées à une fonction pour laquelle elles ont été conçues, par exemple la clé du code d'authentification du message. Les clés étant entrées sous forme chiffrée dans les fonctions cryptographiques, ou extraites en clair d'un emplacement sûr du dispositif cryptographique, la séparation des clés peut être obtenue en faisant varier le procédé sous lequel elles sont chiffrées ou enregistrées.

8.2 Prévention de la substitution

La prévention de la substitution des clés fait obstacle à l'utilisation de clés destinées à une fonction spécifique par des parties autres que celles autorisées ou à des moments non prévus, par exemple, une clé ne peut être utilisée ni par une personne non autorisée, ni après l'expiration de son délai de validité.

8.3 Identification

L'identification de clé permet au destinataire d'une transaction d'identifier la ou les clés associées à la transaction.

8.4 Synchronisation (disponibilité)

La synchronisation cryptographique permet l'utilisation de la clé appropriée, par le donneur d'ordre et par le destinataire, en cas de changement de clé.

8.5 Intégrité

Le contrôle de l'intégrité de la clé consiste à vérifier que la clé n'a pas été altérée.

8.6 Confidentialité

La confidentialité des clés garantit que les clés secrètes ne sont pas divulguées.

8.7 Détection de compromission

Dans certaines situations, il n'est pas possible d'éviter une compromission de la sécurité, mais les effets négatifs qui en résultent peuvent être évités ou limités si celle-ci est détectée. Les cas de compromission peuvent être détectés par des procédures de contrôle et d'audit.

9 Cycle de vie d'une clé pour les algorithmes cryptographiques symétriques

La gestion de clés inclut la génération des clés appropriées, leur distribution aux destinataires autorisés, leur utilisation par les destinataires autorisés, et leur résiliation lorsqu'elles ne sont plus utiles. La protection des clés en conformité avec les principes de gestion de clés recensés dans l'article 5, s'effectue au cours d'une série d'étapes brièvement décrites ci-dessous. La procédure complète est appelée le cycle de vie de la clé. (Ce cycle est décrit en détail dans l'ISO 11568-3.)

9.1 Génération

La génération consiste à créer une nouvelle clé pour une utilisation ultérieure.

9.2 Stockage

Le stockage consiste à conserver une clé sous une forme autorisée.

9.3 Sauvegarde

La sauvegarde consiste à stocker une copie protégée d'une clé pendant sa période de vie opérationnelle.

9.4 Distribution et chargement

Le processus de distribution et de chargement d'une clé consiste à transférer une clé dans un dispositif cryptographique sûr, selon une procédure manuelle ou électronique.

9.5 Utilisation

L'utilisation d'une clé désigne son emploi dans le cadre des opérations cryptographiques pour lesquelles elle a été conçue.

9.6 Remplacement

Le remplacement d'une clé par une autre intervient lorsque la clé d'origine a été découverte ou lorsque sa découverte est probable ou lorsqu'elle arrive en fin de vie opérationnelle.

9.7 Destruction

La destruction d'une clé garantit qu'aucun exemplaire de cette clé, sous l'une des formes autorisées, n'existe à un emplacement précis. Néanmoins, les informations pouvant permettre la reconstitution de la clé pour une utilisation ultérieure peuvent subsister à cet endroit.

9.8 Suppression

La suppression d'une clé est le processus par lequel une clé non désirée et toutes les informations susceptibles d'en permettre la reconstitution sont détruites aux points d'utilisation/stockage. Une clé peut être supprimée sur un emplacement et continuer d'exister sur un autre, pour l'archivage par exemple.

9.9 Archivage

L'archivage d'une clé désigne le stockage d'une clé qui n'est plus opérationnelle sur aucun emplacement.

9.10 Résiliation

Une clé est résiliée lorsqu'elle ne remplit plus aucune fonction et que tous ses exemplaires, ainsi que les informations susceptibles d'en permettre la régénération ou la reconstitution, ont été supprimés de tous les emplacements où ils ont existé.