NORME INTERNATIONALE

ISO 11568-4

Première édition
1998-07-15

Banque — Gestion de clés (services aux particuliers) —

Partie 4:
Techniques de gestion de clés utilisant la cryptographie à clé publique

Banking — Key management (retail) —
Part 4: Key management techniques using public key cryptography

Numéro de référence
ISO 11568-4:1998(F)

Sommaire

Organisation internationale de normalisation
Case postale 56 • CH-1211 Genève 20 • Suisse
Internet iso@iso.ch

Version française tirée en 1999

Imprimé en Suisse

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 11568-4 a été élaborée par le comité technique ISO/TC 68, *Banque, valeurs mobilières et autres services financiers*, sous-comité SC 6, *Services financiers liés à la clientèle*.

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 utilisant les systèmes cryptographiques à clé publique*

— *Partie 5: Cycle de vie des clés pour les systèmes cryptographiques à clé publique*

— *Partie 6: Schémas de gestion de clés*

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

Introduction

L'ISO 11568 décrit les procédures de gestion sécurisée de clés cryptographiques utilisées pour protéger les messages dans le cadre des services bancaires aux particuliers, notamment les messages échangés entre un acquéreur et un dispositif d'acceptation de carte d'une part, et entre un acquéreur et un émetteur de carte d'autre part. La gestion des clés utilisées dans un environnement de cartes à circuit intégré (ICC) n'est pas couverte par l'ISO 11568.

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 norme prescrit les exigences de gestion de clés, applicables dans des domaines ouverts que 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).

L'ISO 11568 est une norme en plusieurs parties.

La présente partie de l'ISO 11568 décrit les techniques de gestion de clés à utiliser dans le cadre des systèmes cryptographiques à clé publique et qui, combinées avec ces derniers, permettent d'assurer les services de gestion de clés décrits dans l'ISO 11568-1. Ces services sont les suivants:

— séparation de clés;

— prévention de la substitution de clés;

— identification de clés;

— synchronisation de clés;

— intégrité des clés;

— confidentialité des clés;

— détection de la découverte de clés.

Banque — Gestion de clés (services aux particuliers) —

Partie 4:
Techniques de gestion de clés utilisant la cryptographie à clé publique

1 Domaine d'application

La présente partie de l'ISO 11568 spécifie les techniques pour l'utilisation et la protection des clés cryptographiques des systèmes cryptographiques à clé publique, dans le cadre des services bancaires aux particuliers.

Elle s'applique à tout organisme responsable de la mise en œuvre de procédures de protection de clés au cours du cycle de vie. Les techniques décrites dans la présente partie de l'ISO 11568 assurent la conformité aux principes décrits dans l'ISO 11568-1.

NOTE La protection requise à chaque étape du cycle de vie des clés, dans le cadre des systèmes cryptographiques à clé publique, est décrite en détails dans l'ISO 11568-5.

Les systèmes cryptographiques à clé publique couvrent les algorithmes cryptographiques asymétriques, les systèmes de signature numérique et les systèmes de distribution de clé publique. Quoique la présente partie de l'ISO 11568 décrive des techniques utilisant ces systèmes dans le cadre particulier de la gestion de clés, certaines de ces techniques peuvent également s'appliquer à la gestion sécurisée de données.

Les techniques sont décrites pour les systèmes cryptographiques à clé publique génériques. Les informations concernant un système en particulier sont données dans une annexe.

Les algorithmes dont l'utilisation avec les techniques décrites dans la présente partie de l'ISO 11568 est approuvée, ainsi que les procédures de leur approbation, sont donnés dans l'annexe A.

L'annexe B contient une présentation normative de la gestion de certificat de clé publique.

L'annexe C contient une description des certificats d'attributs, une technique qui permet d'optimiser la fonctionnalité des certificats de clé publique.

L'annexe D contient une introduction aux trois types de systèmes cryptographiques à clé publique mentionnés ci-dessus.

2 Références normatives

Les normes suivantes contiennent 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 leur publication, les éditions indiquées étaient 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 les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO/CEI 8824:1990, *Technologies de l'information — Interconnexion de systèmes ouverts — Spécification de la notation de syntaxe abstraite numéro 1 (ASN.1).*

ISO/CEI 8825:1990, *Technologies de l'information — Interconnexion de systèmes ouverts — Spécification de règles de base pour coder la notation de syntaxe abstraite numéro UNE (ASN.1).*

ISO 8908:1993, *Banque et services financiers connexes — Vocabulaire et éléments de données.*

ISO/CEI 9594-8:1990, *Technologies de l'information — Interconnexion de systèmes ouverts — L'Annuaire — Partie 8: Cadre général d'authentification.*

ISO/CEI 9796:1991, *Technologies de l'information — Techniques de sécurité — Schéma de signature numérique rétablissant le message*.

ISO 9807:1991, *Banques et services financiers liés aux opérations bancaires — Spécifications liées à l'authentification des messages (service aux particuliers)*.

ISO/CEI 10116:1997, *Technologies de l'information — Techniques de sécurité — Modes opératoires d'un chiffrement par blocs de n-bits.*

ISO/CEI 10118 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Fonctions de brouillage*.

ISO 11166 (toutes les parties), *Banque — Gestion des clés au moyen d'algorithmes asymétriques.*

ISO/CEI 11770-3:—[1)], *Technologies de l'information — Techniques de sécurité — Gestion de clés — Partie 3: Mécanismes utilisant des techniques asymétriques.*

ISO 13491-1:—[1)], *Banque — Dispositifs cryptographiques de sécurité (service aux particuliers) — Partie 1: Concepts, prescriptions et méthodes d'évaluation.*

ANSI X9.30.1:1995, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry — Part 1: The Digital Signature Algorithms (DSA).*

ANSI X9.30.2:1993, *Public Key Cryptography — Part 2*.

AS 2805-5.3, *Ciphers — DEA 2*.

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 asymétrique
algorithme cryptographique dans lequel la clé de chiffrement et la clé de déchiffrement sont différentes, et où il est impossible d'un point de vue informatique de déduire la clé de déchiffrement à partir de la clé de chiffrement

3.2
paire de clés asymétriques
clé publique et clé privée correspondante créées et utilisées au moyen d'un système cryptographique à clé publique

3.3
certificat
pièces d'identité (habilitations) d'une entité, signées à l'aide de la clé privée de l'autorité de certification qui les a émises, en conséquence de quoi elles sont infalsifiables

---

[1)] À publier.

3.4
autorité de certification (CA)
centre de confiance habilité à créer et à attribuer des certificats

NOTE A titre facultatif, l'autorité de certification peut créer et attribuer des clés aux entités.

3.5
impossible d'un point de vue informatique
propriété selon laquelle un calcul est théoriquement réalisable mais est impossible étant donné le temps ou les ressources nécessaires pour l'effectuer avec la puissance actuelle ou prévue des ordinateurs

3.6
pièces d'identité
données d'identification de clé pour une entité, intégrant au moins le nom distinctif de l'entité et sa clé publique

NOTE Des données supplémentaires peuvent y être ajoutées.

3.7
signature numérique
transformation cryptographique d'une donnée permettant au destinataire de cette donnée d'en prouver l'origine et l'intégrité, et servant à protéger l'expéditeur contre la contrefaçon par des tiers ou le destinataire

3.8
système de signature numérique
système cryptographique à clé publique permettant la création puis la vérification des signatures numériques

3.9
fonction de hachage

fonction unidirectionnelle qui fait correspondre un ensemble de chaînes arbitraires avec un ensemble de chaînes de bits de longueur fixe

NOTE Une fonction de hachage résistante à la collision se caractérise par le fait qu'il est impossible d'un point de vue informatique de faire correspondre des données d'entrée distinctes avec la même donnée de sortie.

3.10
accord de clé
établissement d'une clé secrète commune sans référence à une autre clé secrète commune

3.11
propriétaire d'une paire de clés
partie à laquelle appartient la paire de clés

3.12
non-répudiation de l'origine
propriété selon laquelle l'émetteur d'un message et de la valeur de contrôle cryptographique associée (signature numérique) ne peut renier par la suite, avec un niveau acceptable de crédibilité, le fait d'avoir émis le message

3.13
système cryptographique à clé publique
système cryptographique composé de deux opérations complémentaires utilisant chacune une clé prise parmi deux clés distinctes mais liées l'une à l'autre, la clé publique et la clé privée, et doté de la propriété selon laquelle il est impossible d'un point de vue informatique de déterminer la clé privée à partir de la clé publique

3.14
système de distribution de clé publique
système cryptographique à clé publique permettant à deux entités en communication de créer ensemble une clé secrète

3.15
utilisateur de clé publique
partie utilisant la clé publique d'une autre partie pour un service cryptographique

NOTE L'autorité de certification n'est pas un utilisateur de clé publique.

4 Utilisation des systèmes cryptographiques à clé publique dans le cadre des systèmes de services bancaires aux particuliers

Dans les systèmes de services bancaires aux particuliers, les systèmes cryptographiques à clé publique sont utilisés avant tout pour la gestion des clés. Tout d'abord, pour la gestion des clés des algorithmes cryptographiques symétriques, puis pour la gestion des clés des systèmes cryptographiques à clé publique eux-mêmes. Le présent article décrit ces applications des systèmes cryptographiques à clé publique. Les techniques sous-jacentes à ces applications sont décrites dans l'article 5.

4.1 Distribution des clés symétriques

La distribution d'une ou plusieurs clés d'un algorithme cryptographique symétrique peut se faire par transport de clé ou par accord de clé.

NOTE Les mécanismes de distribution des clés symétriques sont décrits dans l'ISO/CEI 11770-3, où la distribution de clé est appelée «établissement de clé».

4.1.1 Transport de clé

Lorsque le transport de clé est utilisé, les clés symétriques doivent être chiffrées à l'aide d'un algorithme cryptographique asymétrique, et le bloc de clés chiffrées résultant doit être transmis au destinataire souhaité. Le chiffrement des clés garantit la confidentialité des clés symétriques pendant la distribution; l'authenticité et l'intégrité du bloc de clés ou de la totalité du message transmis peuvent être garanties en signant le bloc ou le message à l'aide d'un système de signature numérique.

Le chiffrement de clé est décrit dans l'article 5.

NOTE L'ISO 11166-1 décrit les protocoles de transport des clés symétriques. Ces protocoles utilisent à la fois le chiffrement de clé et les signatures numériques.

4.1.2 Accord de clé

Lorsque l'accord de clé est utilisé, les clés de l'algorithme cryptographique symétrique doivent être établies à l'aide d'un système de distribution de clé publique (voir annexe D). Le mécanisme utilisé doit garantir l'authenticité des entités en communication.

4.2 Stockage et distribution des clés publiques asymétriques

La clé publique d'une paire de clés asymétriques doit être distribuée à, et stockée par, un ou plusieurs utilisateurs pour être utilisée ultérieurement en tant que clé de chiffrement et/ou clé de vérification de signature ou pour être employée dans un mécanisme d'accord de clé. Bien que cette clé n'ait pas à être protégée contre la divulgation, les procédures de distribution et de stockage doivent garantir la préservation de son authenticité et de son intégrité.

NOTE Certaines applications sont conçues pour que la sécurité requise dépende de la non-divulgation de la clé publique.

L'une des méthodes suivantes peut être utilisée pour garantir l'authenticité et l'intégrité d'une clé publique pendant son stockage ou sa distribution:

— signature de la clé publique et des données associées au moyen d'un système de signature numérique, ce qui crée un certificat de clé. Les certificats de clé, ainsi que la gestion des clés utilisées pour créer et vérifier les certificats, sont décrits en 5.3 et dans l'article 6;

— création d'un MAC pour la clé publique et les données associées, au moyen de l'algorithme défini dans l'ISO 9807 et d'une clé utilisée exclusivement à cet effet;

— chiffrement de la clé publique et des données associées, au moyen d'un algorithme cryptographique symétrique ou asymétrique.

Le chiffrement de clé est décrit en 5.2.

La méthode complémentaire suivante peut être utilisée pour garantir l'authenticité et l'intégrité d'une clé publique pendant la distribution uniquement:

— distribution de la clé publique sur un canal non protégé, et distribution d'une valeur de vérification de la clé publique et des données associées au moyen d'un canal authentifié par double contrôle. La vérification de clé est décrite en 5.5.

4.3 Stockage et transfert des clés privés asymétriques

La clé privée d'une paire de clés asymétriques n'ayant pas besoin d'être transmise à un site autre que celui de l'utilisateur, dans certains cas elle peut être maintenue dans le dispositif cryptographique sûr qui l'a générée. Si elle doit être sortie du dispositif qui l'a générée (par exemple pour être transmise à un autre dispositif cryptographique sûr où elle doit être utilisée ou à des fins de sauvegarde), elle doit être protégée contre toute découverte à l'aide d'au moins une des techniques ci-dessous:

— chiffrement à l'aide d'une autre clé cryptographique (voir 5.2);

— division en deux ou plusieurs éléments, de manière que chaque bit de la clé protégée dépende de tous les éléments;

— transmission vers un autre dispositif cryptographique sûr, qui est le dispositif cryptographique sûr où elle doit être utilisée, ou vers un dispositif de transmission sûr prévu à cet effet. (Si la voie de communication n'est pas totalement sécurisée, le transfert ne doit être autorisé que dans un environnement sûr.)

5 Techniques de fourniture de services de gestion de clés

Le présent article décrit les techniques pouvant être utilisées, individuellement ou collectivement, pour assurer les services de gestion de clé présentés dans l'ISO 11568-1. Certaines techniques permettent d'assurer plusieurs services de gestion de clé.

Il est souvent nécessaire (ou souhaitable) d'utiliser une paire de clés publiques à plusieurs fins, par exemple pour les signatures numériques et le chiffrement. Dans ces cas, on doit utiliser des techniques de séparation de clés qui garantissent que le système est protégé contre une attaque par des transformations utilisant la paire de clés.

Les techniques choisies doivent être mises en œuvre dans un dispositif cryptographique sûr. La fonctionnalité du dispositif cryptographique doit assurer qu'une technique est mise en œuvre de manière telle que le but fixé de cette technique est atteint.

Les caractéristiques et exigences de gestion d'un dispositif cryptographique sûr sont définies dans l'ISO 13491-1.

5.1 Génération d'une paire de clés asymétriques

Les deux clés d'une paire de clés asymétriques sont mathématiquement liées de la manière définie dans la conception du système cryptographique à clé publique considéré. La relation est telle qu'il est impossible d'un point de vue informatique de déterminer la clé privée à partir de la clé publique.

La plupart des systèmes cryptographiques à clé publique sont basés sur l'arithmétique modulaire. La taille du module détermine non seulement la taille des données et celle des blocs de clés, mais également la difficulté à rompre le système. Lorsque la solidité du système est directement liée à la taille du module, ce dernier doit être choisi de taille suffisante pour rendre les attaques impossibles d'un point de vue informatique.

Tout en garantissant l'existence de la relation requise entre les deux clés, la génération de clé doit utiliser un processus aléatoire ou pseudo-aléatoire tel qu'il soit impossible de prédire une clé ou de déterminer que certaines clés sont, de façon significative, plus probables que d'autres dans l'espace des clés possibles.

NOTE Dans certains systèmes cryptographiques, il est possible d'utiliser une valeur constante connue en tant que partie de la clé publique. Ceci n'est pas incompatible avec l'exigence énoncée ci-dessus.

5.2 Chiffrement de clé

Le chiffrement de clé est une technique selon laquelle une clé est chiffrée au moyen d'une autre clé. La clé chiffrée résultante peut alors être gérée de manière sécurisée (sa confidentialité et/ou son authenticité étant garanties) en dehors d'un dispositif cryptographique sûr. Une clé utilisée pour effectuer ce type de chiffrement est une clé de chiffrement de clé (KEK).

Il existe trois cas différents de chiffrement de clé faisant intervenir les clés et les algorithmes cryptographiques asymétriques décrits ici, dénommés

a) chiffrement d'une clé symétrique à l'aide d'un algorithme cryptographique asymétrique;

b) chiffrement d'une clé asymétrique à l'aide d'un algorithme cryptographique asymétrique;

c) chiffrement d'une clé asymétrique à l'aide d'un algorithme cryptographique symétrique.

NOTE Le chiffrement de clé symétrique à l'aide d'un algorithme cryptographique symétrique est traité dans l'ISO 11568-2.

Bien que le chiffrement de clé garantisse la préservation de la confidentialité de la clé, d'autres techniques peuvent être nécessaires en association avec le chiffrement de clé pour garantir une bonne séparation des clés, par exemple l'étiquetage des clés (voir 5.4).

5.2.1 Chiffrement de clé symétrique à l'aide d'un algorithme cryptographique asymétrique

Le chiffrement d'une clé symétrique à l'aide de la clé publique d'un algorithme cryptographique asymétrique est généralement utilisé pour la distribution de la clé en question au moyen d'un canal non sécurisé. La clé chiffrée peut être une clé de travail ou une KEK. De la sorte, il est possible de créer des hiérarchies de clés composites intégrant des clés d'algorithmes cryptographiques symétriques et asymétriques.

NOTE Les hiérarchies de clés sont décrites dans l'ISO 11568-2.

La clé symétrique doit être formatée de manière à former un bloc de données convenant à l'opération de chiffrement. Les blocs utilisés pour les algorithmes cryptographiques asymétriques ont tendance à dépasser en taille les clés utilisés pour les algorithmes cryptographiques symétriques. C'est pourquoi il est généralement possible d'intégrer plusieurs clés dans le bloc de données utilisé pour le chiffrement. En outre, des informations de formatage, des caractères de remplissage aléatoires et des caractères de redondance peuvent être intégrés dans le bloc de données.

5.2.2 Chiffrement de clé asymétrique à l'aide d'un algorithme cryptographique asymétrique

La clé publique ou la clé privée d'un algorithme cryptographique asymétrique peut elle-même être chiffrée à l'aide d'un algorithme cryptographique asymétrique.

5.2.3 Chiffrement de clé asymétrique à l'aide d'un algorithme cryptographique symétrique

La clé publique ou la clé privée d'un algorithme cryptographique asymétrique peut devoir être chiffrée à l'aide d'un algorithme cryptographique symétrique.

Les clés des algorithmes cryptographiques asymétriques ont tendance à dépasser en taille les blocs utilisés pour les algorithmes cryptographiques symétriques. C'est pourquoi la clé asymétrique doit être formatée de manière à former plusieurs blocs de données de chiffrement. Par conséquent, le mode de fonctionnement par chaînes de blocs de chiffrement doit être utilisé pour le processus de chiffrement.

NOTE 1 Les modes de fonctionnement pour un algorithme cryptographique utilisant des blocs de n bits sont normalisés dans l'ISO/CEI 10116.

Des clés de longueur double doivent être utilisées pour le chiffrement des clés privées asymétriques.

NOTE 2 Le chiffrement utilisant une clé de longueur double est décrit dans l'ISO 11568-2.