NORME INTERNATIONALE

ISO 11568-6

Première édition
1998-07-15

Banque — Gestion de clés (services aux particuliers) —

Partie 6:
Schémas de gestion de clés

Banking — Key management (retail) —
Part 6: Key management schemes

(F)

Sommaire

Page

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

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 11568-6 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 de la présente partie de l'ISO 11568 sont données uniquement à titre d'information.

Introduction

L'ISO 11568 fait partie d'un ensemble de normes décrivant 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 accepteur 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, 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 norme 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).

L'ISO 11568 est une norme en plusieurs parties.

La présente partie de l'ISO 11568 fournit des informations générales et des critères concernant les schémas de gestion de clés à utiliser dans le cadre des services bancaires aux particuliers. L'annexe A contient une description de certains schémas de gestion de clés, que les membres de l'ISO considèrent adaptés au domaine des services bancaires aux particuliers.

Banque — Gestion de clés (services aux particuliers) —

Partie 6:
Schémas de gestion de clés

1 Domaine d'application

La présente partie de l'ISO 11568 contient des descriptions de schémas de gestion de clés qui ont été présentés par les organismes nationaux de normalisation des pays membres comme pouvant convenir à la mise en œuvre dans le cadre des services bancaires aux particuliers.

Chaque description a uniquement pour but de donner un aperçu du schéma de gestion de clé considéré. A cet effet, elle met en évidence les principales caractéristiques du schéma, les techniques particulières employées et d'autres informations utiles.

De plus amples informations concernant ces schémas peuvent être trouvées dans les documents cités en référence dans chaque description.

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

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

ISO/CEI 9798-3:1993, *Technologies de l'information — Techniques de sécurité — Mécanismes d'authentification d'entité — Partie 3: Authentification d'entité utilisant un algorithme à clé publique*.

ISO/CEI 10118-1:1994*, Technologies de l'information — Techniques de sécurité — Fonctions de brouillage — Partie 1: Généralités*.

ISO/CEI 10118-2:1994*, Technologies de l'information — Techniques de sécurité — Fonctions de brouillage — Partie 2: Fonctions de brouillage utilisant un algorithme de chiffrement par blocs de n bits.*

ISO/CEI 10118-3:1998*, Technologies de l'information — Techniques de sécurité — Fonctions de brouillage — Partie 3: Fonctions de hachage dédiées.*

ISO/CEI DIS 10118-4*, Technologies de l'information — Techniques de sécurité — Fonctions de brouillage — Partie 4: Fonctions de hachage utilisant l'arithmétique modulaire.*

ISO 11166-1:1994, *Banque — Gestion des clés au moyen d'algorithmes asymétriques — Partie 1: Principes, procédures et formats*.

ISO 11166-2:1994, *Banque — Gestion des clés au moyen d'algorithmes asymétriques — Partie 2: Algorithmes approuvés utilisant le système de cryptographique RSA.*

ISO 11568-1:1994, *Banque — Gestion de clés (services aux particuliers) — Partie 1: Introduction à la gestion de clés.*

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

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

ISO 13491-2:—[1)], *Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) — Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les systèmes de cartes à bande magnétique.*

3 Définitions

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

4 Présentation générique des schémas de gestion de clés dans le cadre des services bancaires aux particuliers

Un schéma de gestion de clés est un ensemble de règles qui définissent la manière de créer, de distribuer, d'utiliser et de remplacer les clés cryptographiques utilisées dans les systèmes de services bancaires aux particuliers.

L'objectif d'un schéma de gestion de clés est de garantir que les clés cryptographiques sont gérées de manière que les données à protéger soient préservées de tout danger lié à la création, au transfert, à l'utilisation ou au remplacement non sécurisé de clés cryptographiques.

Pour atteindre cet objectif, les schémas de gestion des clés doivent utiliser les techniques de gestion de clés décrites dans l'ISO 11568-2 et l'ISO 11568-4.

Des dispositifs cryptographiques sûrs, décrits dans l'ISO 13491, doivent être utilisés pour assurer le niveau de sécurité recherché.

Les spécifications et la mise en œuvre des phases du cycle de vie des clés cryptographiques sont traitées dans l'ISO 11568-3 et dans l'ISO 11568-5.

Les schémas de gestion de clés peuvent utiliser des techniques symétriques, asymétriques ou hybrides.

Tout schéma de gestion de clés doit respecter les principes de gestion de clés énoncés dans l'ISO 11568-1.

5 Liste des schémas de gestion de clés

Les schémas de gestion de clés ci-dessous sont décrits dans l'annexe A de la présente partie de l'ISO 11568.

— A.1 Schéma de gestion de clés interbancaires (France)

— A.2 Schéma de gestion de clés de transaction (Royaume-Uni)

— A.3 Schéma de clé unique dérivée par transaction (Etats-Unis)

[1)] À publier.

— A.4 Norme de sécurité de base télématique (Suisse)

— A.5 Gestion de clés du terminal à l'acquéreur — Clés de transaction (Australie)

— A.6 Gestion de clés nœud à nœud — Clés de session (Australie)

— A.7 Gestion de clés du terminal à l'acquéreur — Clés de session (Australie)

— A.8 Initialisation de l'unité cryptographique du terminal à l'aide de l'algorithme cryptographique asymétrique (Australie)

Annexe A
(informative)

Description des schémas de gestion de clés

A.1 Schéma de gestion de clés interbancaires

SERVICES BANCAIRES AUX PARTICULIERS — SCHEMAS DE GESTION DE CLES (à utiliser avec l'ISO 11568-6)
NOM DU SCHEMA DE GESTION DE CLES: *Schéma de gestion de clés interbancaires*
SOUMIS PAR: *AFNOR* (France)
ALGORITHME(S) ASSOCIE(S): *DEA*
DESCRIPTION DU SCHEMA: Clé maîtresse. Clés de raccordement: la cryptopériode dure plusieurs années. Clés de chiffrement de clés: ceci est une couche facultative de la hiérarchie de clés, à utiliser dans les systèmes à grand volume. La cryptopériode dure 3 fois la cryptopériode des clés de données — moins un jour. Elle dure au maximum 3 mois. Clés de données (= clés de session): générées automatiquement et distribuées tous les «n» jours — 31 jours au maximum. Ces clés sont les suivantes: clé de chiffrement du PIN clé de MAC NOTE Cette mise en œuvre est une variante de Clé maîtresse / Clé de session.
MISES EN ŒUVRE CONNUES: réseau interbancaire français
REFERENCES TECHNIQUES: Groupement Cartes Bancaires STUR RCB

A.2 Schéma de gestion de clés de transaction

SERVICES BANCAIRES AUX PARTICULIERS — SCHEMAS DE GESTION DE CLES (à utiliser avec l'ISO 11568-6)
NOM DU SCHEMA DE GESTION DE CLES: *CLÉ DE TRANSACTION APACS 40*
SOUMIS PAR: *APACS, ROYAUME-UNI*
ALGORITHME(S) ASSOCIE(S): *DEA* (défini dans ANSI X3.92)
DESCRIPTION DU SCHEMA: Ce schéma réalise les fonctions suivantes: a) authentification de message — en produisant des MAC à 32 bits conformes à l'ANSI X9.19. b) chiffrement du PIN — à l'aide d'un format de bloc PIN/PAN conforme à l'ANSI X9.8. Gestion de clés Des clés distinctes sont utilisées pour les deux fonctions. Les clés sont mises à jour pour chaque transaction, à l'aide des données de la carte, d'un registre des clés et d'une fonction unidirectionnelle. Le registre des clés est mis à jour sur le terminal et sur le système hôte à l'aide de la partie non utilisée du MAC (résidu). Les messages d'une transaction donnée sont reliés en prenant en compte dans le calcul du MAC la partie non utilisée du MAC provenant du message précédent. La protection bout-en-bout et "break forward" des codes PIN peut être obtenue en omettant certaines données de la carte contenues dans les messages transmis. NOTE Cette mise en œuvre est une variation de Clé unique par transaction transformée de manière irréversible.
MISES EN ŒUVRE CONNUES: ROYAUME-UNI
REFERENCES TECHNIQUES: Norme APACS 40*: Spécifications de l'interface de l'acquéreur pour les terminaux de capture de données électroniques: Partie 3, Section 3 — Sécurité*.