NORME INTERNATIONALE

ISO 13492

Première édition
1998-05-15

Banque — Élément de données lié à la gestion des clés (services aux particuliers)

Banking — Key management related data element (retail)

(F)

Sommaire

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 13492 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.*

Les annexes A et B de la présente Norme internationale sont données uniquement à titre d'information.

Introduction

La présente Norme internationale décrit la structure et le contenu d'un élément de données lié à la gestion de clés qui peut être transporté dans des messages transmis de manière électronique dans un environnement de services bancaires aux particuliers, afin de permettre la gestion sûre des clés cryptographiques, cet environnement incluant les communications entre un dispositif d'acceptation de cartes et un acquéreur, et entre un acquéreur et un émetteur de cartes. La gestion de clés utilisées dans une carte à circuit intégré et les éléments de données qui y sont liés ne sont pas couverts par la présente Norme internationale.

La présente Norme internationale offre une compatibilité avec les normes ISO existantes relatives aux messages émis par cartes bancaires (voir ISO 8583).

Banque — Élément de données lié à la gestion des clés (services aux particuliers)

1 Domaine d'application

La présente Norme internationale décrit un élément de données lié à la gestion de clés qui peut être transporté soit dans des messages de transactions pour transporter des informations sur les clés cryptographiques utilisées pour sécuriser la transaction en cours, soit dans des messages de service cryptographique pour transporter des informations sur les clés cryptographiques à utiliser pour sécuriser des transactions ultérieures.

La présente Norme internationale traite les exigences liées à l'utilisation des éléments de données liés à la gestion de clés de l'ISO 8583, en utilisant les deux éléments de données suivants de l'ISO 8583: l'Information de Contrôle Liée à la Sécurité (bit 53) ou la Donnée de Gestion de Clés (bit 96). Néanmoins, le transport de données lié à la gestion de clés n'est pas limité à l'ISO 8583.

La présente Norme internationale est applicable aux systèmes de relations cryptographiques symétriques ou asymétriques.

Les procédures de gestion de clés, applicables à une gestion sûre des clés cryptographiques dans le cadre des services bancaires aux particuliers, sont décrites dans l'ISO 11568. Des données liées à la sécurité, telles que le numéro d'identification personnel (PIN) et le code d'authentification de messages (MAC), sont respectivement décrites dans l'ISO 9564 et l'ISO 9807.

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 Norme internationale. 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 Norme internationale 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 7812-1:1993, *Cartes d'identification — Identification des émetteurs — Partie 1: Système de numérotation.*

ISO/CEI 7812-2:1993, *Cartes d'identification — Identification des émetteurs — Partie 2: Procédures de demande d'enregistrement.*

ISO 8583:1993, *Messages initiés par carte de transaction financière — Spécifications d'échange de messages.*

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

ISO 9564-1:1991, *Banque — Gestion et sécurité du numéro personnel d'identification — Partie 1: Principes et techniques de protection du PIN.*

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

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

ISO 11568-2:1994, *Banque — Gestion de clés (services aux particuliers) — Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques.*

ISO 11568-3:1994, *Banque — Gestion de clés (services aux particuliers) — Partie 3: Cycle de vie des clés pour les algorithmes cryptographiques symétriques.*

ANSI X3.92:1987, *Data Encryption Algorithm*.

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions données dans l'ISO 8908 et les définitions suivantes s'appliquent.

3.1
relation cryptographique asymétrique
type de relation cryptographique dans laquelle les clés de chiffrement et de déchiffrement sont différentes, et pour lesquelles il est impossible par un calcul sur ordinateur de déduire la clé de déchiffrement à partir de la clé de chiffrement

3.2
relation cryptographique
paire d'opérations qui effectue des transformations entre un texte en clair et un texte chiffré sous le contrôle d'un paramètre appelé clé

NOTE L'opération de chiffrement transforme les données (texte en clair) sous une forme inintelligible (texte chiffré). L'opération de déchiffrement rétablit le texte original.

3.3
algorithme cryptographique
ensemble de règles spécifiant les procédures à appliquer pour le chiffrement et pour le déchiffrement des données

NOTE 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.

3.4
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

3.5
message de service cryptographique
message destiné au transport des clés ou des informations utilisées pour le contrôle d'une relation mettant en jeu des clés

3.6
clé primaire
clé de transaction à partir de laquelle les autres clés de la transaction sont produites (par exemple au moyen de variantes ou de transformations)

3.7
relation cryptographique symétrique
type de relation cryptographique utilisant la même clé secrète pour le chiffrement et le déchiffrement

3.8
message de transaction
message utilisé pour transporter des informations liées à une transaction financière

4 Exigences pour les données liées à la gestion de clés

Un élément de données lié à la gestion de clés qui transporte de l'information sur la (les) clé(s) associée(s) à la transaction est normalement subdivisé en sous champs. Cet élément de données peut être transmis dans une transaction où la nature des sous champs est implicitement connue des parties en communication. Dans de tels environnements, les parties peuvent utiliser l'élément de données lié à la gestion de clés comme un champ d'usage privé et définir ses sous champs de n'importe quelle façon mutuellement admise. Dans d'autres environnements, des transactions sont échangées où la nature des sous champs n'est pas implicitement connue et pour cela doivent être structurés en utilisant une représentation normalisée afin de permettre l'interopérabilité. Dans encore d'autres environnements, les deux types de transactions peuvent être échangées.

Pour faire la distinction entre les transactions où l'élément de données lié à la gestion de clés doit avoir une représentation normalisée et celles où il est utilisé pour un usage privé, le premier octet de l'élément de données lié à la gestion de clés doit être structuré comme un « octet de contrôle » défini de la manière suivante:

00-9F: Le premier sous champ de l'élément des données lié à la gestion de clés est un «identifiant de jeu de clés» de longueur variable, tel que défini en 4.1 et 4.2.

A0-FF: L'élément de données lié à la gestion des clés est un champ d'usage privé, où la nature des sous-champs est implicitement connue des deux entités en communication.

L'utilisation d'identifiants de jeu de clés fournit un moyen normalisé de transporter n'importe quel type d'information liée à la sécurité associé à n'importe quel type de système de gestion de clés. Cette approche élimine le besoin d'identifier des techniques spécifiques de gestion de clés et de définir des sous champs spécifiques afin de s'adapter aux besoins de chacune de ces techniques.

Lorsque l'élément de données lié à la gestion des clés commence par un identifiant de jeu de clés, la partie non utilisée de l'élément de données fournit les différents types d'informations nécessaires au jeu de clés associé pour déterminer la ou les clé(s) nécessaire(s) au traitement cryptographique de cette transaction. En conséquence, il n'y a pas de structure spécifique pour les sous champs contenus dans le reste de l'élément de données. Toute information qui peut varier d'une transaction à l'autre est transmise selon le principe des identifiants de jeu de clés. Cette information inclut normalement l'identité de la clé spécifique à ce jeu de clés.

Les informations liées à la gestion des clés qui ne changent pas d'une transaction à l'autre n'ont pas besoin d'être transmises dans chaque transaction. Mieux, elles peuvent être implicitement connues, ou installées simultanément avec les clés correspondantes et enregistrées avec celles-ci. Des exemples d'informations qui peuvent être implicitement connues sont les suivants.

— La technique de gestion de clés utilisée pour les clés de transaction (clé statique, clé unique par transaction).

— Le format des données chiffrées ou authentifiées (format de PIN bloc).

— L'algorithme de chiffrement utilisé.

— Le nombre de clés utilisées avec la transaction et la fonction de chacune.

Dans certains schémas de gestion de clés, il peut être inutile de transmettre l'élément de données lié à la gestion de clés dans le message de transaction. Le besoin de transmettre un tel élément de données est abordé dans l'annexe A.

4.1 Le concept d'identifiants de jeu de clés

Un identifiant de jeu de clés est un nombre qui identifie un jeu de clés de façon unique; un jeu de clés est un groupe de clés liées entre elles; elles sont toutes différentes, mais ont certaines caractéristiques en commun, en particulier les suivantes.

— Elles sont toutes gérées selon la même méthode de gestion de clés.

— La même clé de haut niveau est utilisée pour chiffrer (pour un enregistrement en base de données) ou pour dériver toutes les clés du jeu.

— La partie non utilisée de l'élément de données lié à la gestion de clés (au delà de l'identifiant du jeu de clés) est structurée de façon identique pour toutes les clés du jeu et est interprétée selon la même logique.

Un système logique (c'est-à-dire un logiciel) sur l'ordinateur hôte d'acquisition ayant pour but d'interpréter l'élément de données lié à la gestion des clés doit être associé à tout jeu de clés donné, ceci afin de déterminer quelle clé a été utilisée par la transaction et comment cette clé doit être traitée.

Des jeux de clés multiples, avec différents identifiants de jeu de clés, peuvent utiliser exactement la même logique, se différenciant seulement, par exemple, par la clé de chiffrement ou de dérivation de clé utilisée pour déchiffrer ou dériver la clé de la transaction associée.

Le premier octet de l'identifiant de jeu de clés est l'octet de contrôle (00-9F). Les identifiants de jeu de clés sont affectés comme décrit en 4.2. Les identifiants de jeu de clés sont de longueur variable et n'ont pas de longueur maximum spécifiée. La longueur de l'identifiant de jeu de clés est implicite. En conséquence, l'élément de données lié à la gestion des clés ne doit pas contenir un sous champ de « longueur » précédant l'identifiant de jeu de clés pour indiquer la longueur de celui-ci. De même, il n'est pas nécessaire de faire suivre l'identifiant de jeu de clés d'un délimiteur spécifique. (A noter que si l'élément de données lié à la gestion de clés est transmis dans un champ de longueur variable, il peut être lui-même précédé d'un sous champ de longueur, indiquant la longueur de l'élément de données complet, comme cela est spécifié dans l'ISO 8583 pour les éléments de données « Information de Contrôle Liée à la Gestion de la Sécurité » et « Donnée de Gestion de Clés ».)

Comme les identifiants de jeu de clés sont de longueur variable et que cette longueur est implicite, l'ordinateur hôte d'acquisition devrait stocker, dans la table des identifiants de jeu de clés qu'il gère, la longueur de chacun de ces identifiants. Lorsqu'un hôte reçoit une transaction, par exemple d'un terminal point de vente, il devrait essayer de faire correspondre l'identifiant de jeu de clés aux entrées de ces tables en employant autant de chiffres (les plus à gauche) qu'il en est défini dans l'entrée spécifique de la table pour cet élément de données. Une correspondance indique que cette entrée de table contient l'identifiant de jeu de clés qui s'applique à l'élément de données lié à la gestion de clés qu'il vient de recevoir.

4.2 Affectation d'identifiants de jeu de clés

Pour éviter aux institutions d'affecter des identifiants de jeu de clés identiques, ceux-ci doivent être affectés en utilisant soit leur numéro d'identification d'émetteur à six chiffres (IIN), tel que défini dans l'ISO 7812, soit leur code d'identification d'institution à six chiffres (IIC), tel que défini dans l'ISO 8583. L'autorité d'enregistrement de l'ISO affecte les IIN aux institutions qui émettent des cartes, et les IIC aux institutions qui n'en émettent pas. Comme un IIN ou un IIC est propre à l'institution à laquelle il est attribué, et que ces deux ensembles de nombres ne se recouvrent pas, cela assure que, si deux environnements cryptographiques se combinent, les identifiants de jeu de clés, qui étaient uniques dans chacun des environnements, le sont également dans l'environnement combiné.

Une organisation qui souhaite obtenir un jeu d'identifiant de clés et à qui il n'a pas été affecté de IIN ou de IIC peut également obtenir un tel identifiant d'une institution en ayant reçu. Une telle institution doit s'assurer qu'elle n'affecte pas d'identifiant de jeu de clés déjà existant.

Une institution peut utiliser directement un IIN ou un IIC comme identifiant de jeu de clés, à condition qu'elle n'ait jamais besoin de plus d'identifiants de jeu de clés que le nombre de numéros d'identification qui lui ont été affectés. Si l'institution a besoin d'identifiants supplémentaires, elle peut concaténer un ou plusieurs chiffres hexadécimaux à la droite d'un IIN ou IIC, et de cette manière obtenir des identifiants de jeu de clés multiples à partir d'un seul IIN ou IIC.

L'institution allouant des identifiants de jeu de clés devrait décider, préalablement à l'allocation, combien de chiffres (s'il y en a plusieurs) doivent être concaténés aux IIN ou IIC pour obtenir ses identifiants de jeu de clés, basés sur ces IIN ou IIC. Par exemple, si une institution décide d'utiliser des identifiants de jeu de clés de sept chiffres, en concaténant un seul chiffre au IIN ou IIC, elle ne peut plus, après avoir utilisé tous les 16 nombres de sept chiffres, ajouter un huitième chiffre pour obtenir de nouveaux identifiants de jeu de clés. Un tel identifiant de jeu de clés de huit chiffres correspondrait, au niveau des sept premiers chiffres, à un identifiant de jeu de clés déjà attribué. Par exemple, si l'identifiant de jeu de clés « 1362047 » existe déjà, l'identifiant de jeu de clés « 13620475 » ne peut pas

être attribué, et vice versa, parce que l'un est complètement inclus dans l'autre. Un exemple d'utilisation des identifiants de jeu de clés est donné à l'annexe B.

5 Mise en œuvre dans l'ISO 8583

Lorsque l'élément de données lié à la gestion de clés décrit dans l•article 4 est utilisé avec l'ISO 8583 pour transporter les informations de gestion de clés de la transaction courante, le contenu de cette donnée doit être transmis en utilisant l'Information de Contrôle Liée à la Sécurité de l'ISO 8583, qui est un élément de données binaires de longueur variable pouvant aller jusqu'à 48 octets.

NOTE 1 Des exemples de messages ISO 8583 dans lesquels l'Information de Contrôle Liée à la Sécurité peut être transmise sont la demande financière ou d'autorisation qui contient le numéro d'identification personnel (PIN, bit 52), ou un message de gestion de réseau ou de modification de fichier qui contient le champ d'authentification de message (MAC, bit 64 ou 128).

Lorsque l'élément de données lié à la gestion de clés est utilisé avec l'ISO 8583 dans des messages de services cryptographiques pour transporter les informations de gestion de clés pour un usage futur, le contenu de cette donnée doit être transmis en utilisant la Donnée de Gestion de Clés de l'ISO 8583, qui est un élément de données binaires de longueur variable pouvant aller jusqu'à 999 octets.

NOTE 2 Des exemples de messages ISO 8583 dans lesquels la Donnée de Gestion de Clés peut être transmise sont la demande ou la réponse à la demande de gestion de réseau, soit pour confirmer la synchronisation des clés actuelles, soit pour échanger de futures clés.