NORME INTERNATIONALE

ISO 11568-2

Première édition
1994-12-01

Banque — Gestion de clés (services aux particuliers) —

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

Banking — Key management (retail) —
Part 2: Key management techniques for symmetric ciphers

Numéro de référence
ISO 11568-2:1994(F)

Sommaire

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse
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 11568-2 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*

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

Introduction

L' ISO 11568 fait partie d'un ensemble de normes décrivant des procédures destinées à sécuriser la gestion des clés cryptographiques secrètes qui protègent les messages dans un environnement de services bancaires aux particuliers, par exemple les messages échangés entre un acquéreur et un accepteur de cartes ou entre un acquéreur et un émetteur de cartes. La gestion de 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 ceux des services bancaires aux particuliers. Les autorisations de crédit et de débit aux points de vente/points de service (TPE) et les transactions aux guichets automatiques de banques (GAB) en sont des services typiques.

La présente partie de l'ISO 11568 décrit des techniques de gestion de clés qui peuvent être combinées pour fournir les services de gestion de clés présentées dans l'ISO 11568-1. Ces services sont les suivants :

— séparation des clés
— prévention de la substitution
— identification
— synchronisation
— intégrité
— confidentialité
— détection de la compromission d'une clé

Les techniques associées aux différents services de gestion de clés sont répertoriées dans le tableau figurant à l'article 6.

Banque — Gestion de clés (services aux particuliers) —

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

1 Domaine d'application

La présente partie de l'ISO 11568 prescrit les techniques de protection de clés pour les algorithmes cryptographiques symétriques dans le cadre des services bancaires aux particuliers.

Elle est applicable à toutes les entités chargées de la mise en place de procédures de protection aux différentes étapes du cycle de vie des clés. Les techniques décrites ci-après sont conformes aux principes exposés dans l'ISO 11568-1.

Ces techniques s'appliquent à tous les algorithmes cryptographiques symétriques par blocs de *n* bits.

Les notations employées dans la présente partie de l'ISO 11568 sont répertoriées dans l'annexe A.

L'annexe B fournit la liste des algorithmes approuvés compatibles avec les techniques décrites dans la présente partie de l'ISO 11568.

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 liés aux opérations bancaires — Vocabulaire et éléments de données.*

ISO/CEI 10116:1991, *Technologies de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de n-bits.*

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

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, *Data Encryption Algorithm.*

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 : Désigne l'ensemble des deux opérations inverses de chiffrement et de déchiffrement. Ces opérations utilisent un paramètre appelé «clé». La première transforme le texte initial (texte en clair) de façon à le rendre inintelligible (texte chiffré), et la seconde rétablit le texte initial.

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

3.3 intégrité des données : Qualité des données qui n'ont pas été altérées ou détruites d'une manière frauduleuse.

3.4 clé de données : Clé utilisée pour le chiffrement, le déchiffrement ou l'authentification de données.

3.5 OU exclusif : voir addition modulo-2.

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

3.7 élément de clé : L'un des paramètres généré de façon aléatoire ou pseudo-aléatoire qui a les caractéristiques d'une clé de chiffrement (par exemple pour ce qui concerne le format et la définition aléatoire) et qui est ajouté modulo-2 à un ou plusieurs autres paramètres semblables pour former une clé de chiffrement.

3.8 décalage de clé : Résultat de l'addition modulo-2 d'une clé cryptographique et de la valeur d'un compteur.

3.9 espace de clés : Ensemble de toutes les clés possibles utilisées dans un algorithme cryptographique.

3.10 code d'authentification du message (MAC : Message Authentication Code) : Code inclus dans un message transmis par un donneur d'ordre à un destinataire, permettant de valider la source et tout ou partie du texte du message. Ce code résulte d'un calcul convenu entre les parties concernées.

3.11 addition modulo-2 ; OU exclusif : Addition binaire sans retenue donnant les valeurs suivantes :

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

3.12 algorithme cryptographique par blocs de *n* bits : Algorithme cryptographique par blocs s'appliquant à des blocs de texte (en clair et chiffrés) de *n* bits.

3.13 notarisation : Modification d'une clé de chiffrement de clé de façon à permettre l'authentification du donneur d'ordre et du destinataire final.

3.14 donneur d'ordre : Partie qui est responsable de l'émission d'un message cryptographique.

3.15 pseudo-aléatoire : Désigne un processus statistiquement aléatoire et non prévisible, bien qu'il soit généré par un processus algorithmique.

3.16 destinataire : Partie qui est responsable de la réception d'un message cryptographique.

3.17 dispositif cryptographique sûr : Appareil offrant des garanties de sécurité pour le stockage des données secrètes (telles que des clés) et fournissant des services de sécurité sur la base de ces informations secrètes.

4 Environnement général pour les techniques de gestion de clés

Les techniques utilisables pour rendre les services de gestion de clés sont décrites à l'article 5. Cet article décrit l'environnement dans lequel ces techniques sont mises en œuvre et introduit des concepts fondamentaux et des opérations qui sont communs aux différentes techniques.

4.1 Fonctionnalités d'un dispositif cryptographique sûr

Un algorithme cryptographique symétrique par blocs repose sur les opérations élémentaires de chiffrement et de déchiffrement d'un bloc de données au moyen d'une clé secrète déterminée. Lorsque le traitement porte sur plusieurs blocs de données, ces opérations pourraient utiliser un mode opératoire conforme aux spécifications de la norme ISO 10116. À ce niveau, les données et les clés n'ont aucune signification particulière.

Pour garantir la protection des clés et autres données confidentielles, un dispositif cryptographique sûr doit offrir une interface fonctionnelle de niveau supérieur, chaque opération étant constituée de plusieurs opérations cryptographiques élémentaires utilisant une combinaison de clés et de données fournies par l'interface ou provenant d'un résultat intermédiaire. Ces opérations cryptographiques complexes sont appelées fonctions, chacune ne s'appliquant qu'à un type particulier de données et de clé.

4.1.1 Types de données

La cryptographie au niveau de l'application attribue différentes significations aux données qui sont alors traitées et protégées de façon spécifique dans le dispositif cryptographique sûr. Les données dotées d'une même signification constituent un type de données. Le dispositif cryptographique sûr interdit de manipuler un type de donnée de manière inappropriée.

Par exemple, un numéro personnel d'identification (PIN) représente un type de données dont la confidentialité doit être préservée, alors que d'autres données de transaction peuvent appartenir à un type de données pour lequel seule l'authentification est requise.

Une clé cryptographique peut être considérée comme un type particulier de données. Un dispositif cryptographique sûr garantit qu'une clé ne peut exister que sous l'une des formes autorisées dans l'ISO 11568-3.

4.1.2 Types de clés

Une clé est classée en fonction du type de données sur laquelle elle s'applique et en fonction de son mode de fonctionnement. Le dispositif cryptographique sûr garantit la séparation des clés, de sorte qu'une clé ne puisse être utilisée que pour le type de données approprié et de la façon requise.

Par exemple, une clé de chiffrement du PIN appartient à un type de clé réservé au chiffrement des numéros personnels d'identification alors qu'une clé de chiffrement de clé (KEK) est destinée au chiffrement d'autres clés. Différents types de clés de chiffrement de clé peuvent également être définis, par exemple selon que le chiffrement s'applique aux clés de chiffrement du PIN ou aux clés de MAC.

4.1.3 Fonctions cryptographiques

Le jeu de fonctions supporté par le dispositif cryptographique sûr reflète directement les exigences cryptographiques de l'application telles que chiffrement du PIN, vérification d'un PIN chiffré, génération d'un code d'authentification du message, génération d'une clé aléatoire chiffrée.

Un dispositif cryptographique sûr est conçu de telle manière qu'aucune fonction individuelle ou combinaison de fonctions ne puisse permettre l'obtention illicite d'information sensible. Une conception de ce type est réputée logiquement sûre.

Un dispositif cryptographique sûr peut nécessiter l'usage de différents types de clés. Les clés cryptographiques peuvent être stockées en toute sûreté en dehors du dispositif cryptographique, à condition d'être chiffrées par des clés de chiffrement de clé stockées uniquement à l'intérieur du dispositif, ou elles-mêmes chiffrées au moyen de clés de chiffrement de clé de niveau supérieur.

Une technique pour assurer la séparation des clés peut être l'utilisation d'un type de clé de chiffrement de clé, spécifique pour chaque type de clé. Dans ce cas, lorsqu'une clé chiffrée est transmise au dispositif cryptographique, elle est déchiffrée au moyen du type de clé de chiffrement de clé correspondant au type de clé attendu. Si elle n'appartient pas au type de clé approprié, c'est-à-dire si elle a été chiffrée au moyen d'un autre type de clé de chiffrement de clé, le déchiffrement donne une valeur de clé incorrecte.

4.2 Clé double

La clé secrète utilisée pour un algorithme cryptographique symétrique par blocs peut faire l'objet dans un temps futur d'une attaque par recherche exhaustive, consistant à tester successivement chacune des clés de l'espace de clés jusqu'à trouver la bonne. Pour cela, l'auteur de l'attaque doit connaître un texte chiffré et le texte en clair correspondant (connu ou supposé tel). Il applique alors chaque clé au texte chiffré, et il compare le résultat obtenu avec le texte en clair connu.

Le temps moyen nécessaire à la découverte d'une clé par cette méthode est proportionnel à la taille de l'espace de clés.

Les opérations cryptographiques utilisant une clé double permettent de se prémunir efficacement contre ce type d'attaque. Une clé double est désignée par un astérisque précédant le nom de la clé, *K, par exemple. Elle peut également être désignée sous le nom de paire de clés car elle est formée de la concaténation de deux clés simples : une clé gauche et une clé droite (désignées respectivement par les suffixes «l» et «r»). Ainsi :

$$*K = Kl \,||\, Kr$$

Lorsque le contexte permet d'utiliser indifféremment une clé simple ou double, la notation (*)K est utilisée. Les abréviations utilisées dans la présente partie de l'ISO 11568 sont décrites dans l'annexe C.

Le chiffrement et le déchiffrement d'un bloc simple au moyen d'une clé double sont définis comme indiqué à la figure 1 :

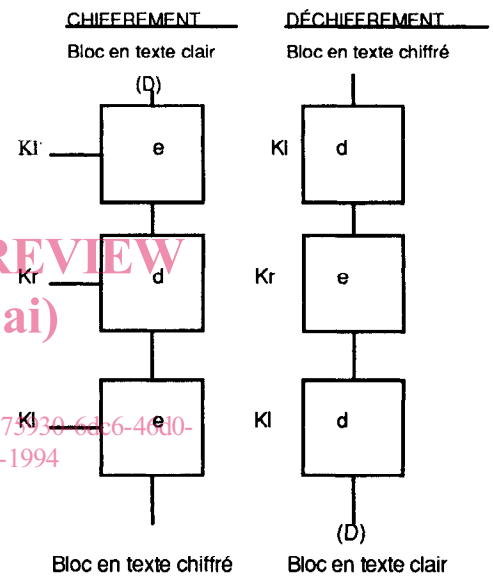

Figure 1 — Utilisation des clés doubles

Cette opération de «triple chiffrement» est souvent désignée par la notation «ede» alors que l'opération inverse de «triple déchiffrement» est désignée par «ded» :

$$ede*K(D) = eKl(dKr(eKl(D)))$$

$$ded*K(D) = dKl(eKr(dKl(D)))$$

Les opérateurs «e» et «d» peuvent aussi désigner implicitement des opérations de chiffrement et de déchiffrement multiples, lorsqu'ils sont appliqués à des clés doubles. Ainsi :

$$e*K(D) = ede*K(D)$$

$$d*K(D) = ded*K(D)$$

Selon les définitions ci-dessus, une clé double dont les clés gauche (l) et droite (r) ont la même valeur est équivalente à une clé simple ayant cette valeur.

4.3 Génération de clé

Les principes de gestion de clés exposés dans l'ISO 11568-1 prescrivent que les clés soient générées selon un processus ne permettant pas de prévoir la valeur de la clé ni d'isoler des valeurs de plus grande probabilité dans l'espace de clés.

À cet effet, les clés et les éléments de clé doivent être générés selon un processus aléatoire ou pseudo-aléatoire, ce dernier pouvant éventuellement être renouvelable.

4.3.1 Génération de clé non renouvelable

La génération de clé non renouvelable peut utiliser une valeur stochastique, telle que produite par un générateur de nombre aléatoire, ou peut résulter d'un processus pseudo-aléatoire.

L'équation ci-dessous illustre la génération d'une clé «Kx» au moyen d'un processus pseudo-aléatoire, où K désigne une clé cryptographique secrète réservée à la génération de clé, V une valeur secrète de diversification et DT un vecteur date-heure mis à jour à chaque génération :

$$Kx = eK\,(eK(DT) \oplus V)$$

Une nouvelle valeur V est générée :

$$V = eK\,(Kx \oplus eK\,(DT))$$

4.3.2 Génération de clé renouvelable

Dans certains cas, il peut être utile de générer une ou plusieurs clés, jusqu'à plusieurs milliers dans certains cas, à partir d'une clé initiale unique, au moyen d'un processus renouvelable. Celui-ci permet de recréer à volonté une clé générée précédemment, et il peut être mis en œuvre à n'importe quel emplacement disposant de la clé de diversification et des données de génération appropriées. Il réduit de manière significative le nombre des opérations manuelles de gestion, de stockage et de distribution de clés.

Le processus de génération de clé doit être conçu de telle sorte que si la clé initiale est imprévisible dans l'espace de clés (conformément aux principes de gestion de clés), il en est de même pour toutes les clés résultantes.

La procédure peut être utilisée de façon itérative toute clé générée à partir d'une clé initiale pouvant elle-même servir de clé initiale pour la génération d'autres clés.

Le processus de génération doit être irréversible, de sorte que la découverte d'une clé générée ne permette pas, celle de la clé initiale ni de toute autre clé générée. Le chiffrement d'une valeur non secrète au moyen de la clé initiale est un exemple de génération de clé.

4.4 Calcul de clé

Il est possible d'obtenir plusieurs clés à partir d'une clé unique au moyen d'un processus réversible, par exemple par l'addition modulo-2 de cette clé et d'une valeur non secrète.

Le calcul de clé est à la fois simple et rapide, mais la découverte d'une clé ainsi calculée entraîne celle de la clé initiale et de toutes les autres clés calculées à partir de celle-ci.

4.5 Hiérarchie de clés

Dans une structure hiérarchique de clés, la confidentialité de certaines clés dépend de celle d'autres clés. Par définition, la découverte d'une clé à un niveau donné de la hiérarchie ne doit pas permettre celle des clés d'un niveau supérieur.

Le chiffrement de clé présente une hiérarchie dans laquelle une clé de chiffrement de clé (KEK) est considérée comme étant d'un niveau supérieur à celui de la clé qu'elle chiffre. La structure hiérarchique de base comporte deux niveaux : les clés de travail sont chiffrées par des clés de chiffrement de clé qui sont stockées dans un dispositif cryptographique. On peut ensuite ajouter un troisième niveau pour le chiffrement des clés de chiffrement de clé par d'autres clés de chiffrement de clé de niveau supérieur, puis un quatrième, etc.

De même, dans le cas d'une clé initiale ou d'une clé de génération de clé (KGK) permettant de produire d'autres clés via un processus déterministe, la clé de génération de clé se trouve à un niveau supérieur à celui des clés qu'elle génère.

En général, les clés qui se trouvent au sommet de la hiérarchie ont une durée de vie longue et assurent la protection d'un grand nombre de clés, pour cela il convient qu'elles soient des clés doubles.

5 Techniques associées aux services de gestion de clés

Les techniques présentées dans cet article peuvent être utilisées seules ou combinées pour permettre la mise en œuvre des services de gestion de clés présentées dans l'ISO 11568-1. Certaines techniques sont employées pour plusieurs fonctions. Le tableau 1 indique quelles sont les techniques associées à chaque service de gestion de clés. Par ailleurs un exemple de schéma de gestion de clés pour un algorithme cryptographique symétrique est présenté dans l'annexe D.

Les techniques retenues doivent être mises en œuvre dans un dispositif cryptographique sûr. Les fonctionnalités du dispositif cryptographique garantissent que la mise en œuvre d'une technique est conforme aux buts recherchés.

5.1 Chiffrement de clé

Le chiffrement de clé est une technique dans laquelle une clé est chiffrée par une autre clé. La clé chiffrée résultante peut alors être gérée de façon sûre à l'extérieur de l'environnement protégé du dispositif cryptographique. La clé utilisée pour chiffrer est appelée clé de chiffrement de clé (KEK).

L'utilisation d'une clé en dehors d'un dispositif cryptographique peut avoir lieu dans les cas suivants :

a) lorsqu'une clé doit être transmise de façon sûre vers un dispositif cryptographique via un canal non protégé ;

b) lorsque les conditions requises pour le stockage de clés d'un nœud dépassent les possibilités du dispositif cryptographique.

En général, les clés de chiffrement de clé ont une durée de vie longue et assurent la protection d'un grand nombre de clés pour cela elles devraient être des clés doubles.

Le chiffrement d'une clé simple par une clé double s'effectue comme indiqué en 4.2, où la clé simple remplace le bloc de texte en clair.

Le chiffrement d'une clé double par une autre clé double requiert le chiffrement séparé des clés gauche et droite, c'est-à-dire

$$*KEK(*K) = e*KEK(Kl) || e*KEK(Kr)$$

Une clé ne devrait jamais être chiffrée par une clé de longueur inférieure. Ainsi, une clé double utilisée avec un algorithme cryptographique donné ne peut être chiffrée par une clé simple de ce même algorithme.

La technique de chiffrement des clés garantit leur confidentialité. Elle peut toutefois être combinée avec d'autres techniques pour assurer la séparation des clés et prévenir leur substitution.

5.2 Variantes de clé

Les variantes d'une clé sont une technique pour obtenir un ensemble de clés à partir d'une clé initiale.

Cette technique permet de réaliser la séparation des clés sans avoir à manipuler une clé distincte et indépendante pour chaque type de clé. Chaque variante d'une clé est calculée à partir de la clé initiale et d'une valeur extraite d'un jeu de constantes non secrètes (voir figure 2), selon un processus renouvelable (f). Ce processus, le calcul de clé, est décrit en 4.4.

À chaque type de clé correspond une constante ayant une valeur spécifique à l'intérieur du jeu de constantes.

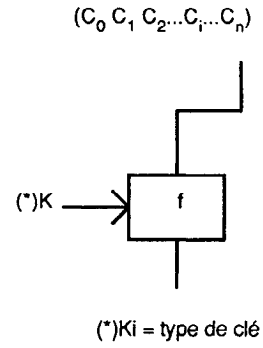

Figure 2 — Calcul d'une variante d'une clé

Une variante calculée au moyen d'un processus réversible doit être conservée exclusivement à l'intérieur du dispositif cryptographique contenant la clé initiale.

La technique des variantes de clé peut être utilisée à tous les niveaux d'une hiérarchie de clés. Ainsi, une clé «de longueur» simple peut être utilisée pour calculer un ensemble de clés de chiffrement de clé, chacune étant destinée au chiffrement d'un type de clé particulier. De même, une clé de longueur simple peut générer un ensemble de clés de travail de différents types.

NOTE 1 Pour plus de précisions sur les variantes de clé et les vecteurs de contrôle, se reporter à l'annexe E.

5.3 Dérivation de clé

La technique de dérivation permet de générer (dériver) plusieurs clés (potentiellement en très grand nombre) à partir d'une seule clé initiale — clé de dérivation — et de données variables non secrètes, chacune des clés produites — clés dérivées — servant de clé initiale dans un dispositif cryptographique sûr particulier (en général le clavier d'entrée du PIN d'un terminal de transfert électronique de fonds au point de vente). La technique de dérivation garantit la séparation des clés en générant une clé (statistiquement) unique pour chaque dispositif, sans qu'il soit nécessaire de gérer un grand nombre de clés distinctes et indépendantes. Ainsi, il n'est pas nécessaire de stocker chaque clé initiale (sous forme chiffrée ou non) au niveau du nœud acquéreur ou destinataire, toute clé dérivée pouvant être générée à n'importe quel moment à partir de la clé de dérivation et des données de dérivation appropriées.

La génération d'une clé dérivée utilise un processus irréversible (voir figure 3), dans lequel interviennent la clé de dérivation et les données associées de façon spécifique au dispositif cryptographique visé.

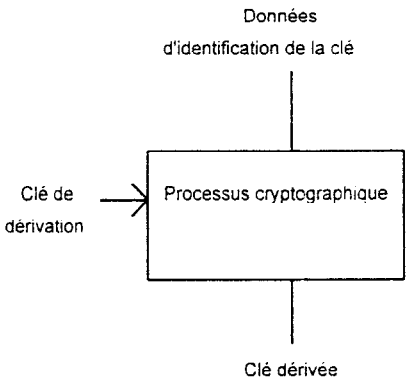

Figure 3 — Génération d'une clé dérivée

Le caractère non réversible du processus garantit que la compromission d'une clé dérivée ne permet pas de découvrir la clé de dérivation ni aucune autre clé dérivée. En revanche, la compromission d'une clé de dérivation entraîne la découverte de toutes les clés dérivées correspondantes.

NOTE 2 La procédure décrite ci-dessus montre qu'une variante d'une clé (voir 5.2) ne peut être considérée comme une clé dérivée.

5.4 Transformation de clé

La technique de transformation de clé permet à un dispositif cryptographique sûr, en général le clavier d'entrée du PIN d'un terminal de transfert électronique de fonds au point de vente de procéder au remplacement d'une clé en générant une ou plusieurs nouvelles clés à partir de la clé en vigueur, puis en supprimant toute trace de cette dernière.

La transformation de clé réduit les conséquences de la découverte d'une clé en permettant au dispositif cryptographique de remplacer ses clés à intervalles rapprochés (par exemple après chaque transaction) sans avoir à recourir à une distribution de clé.

La transformation de clé consiste à utiliser la clé en vigueur comme clé initiale d'un processus irréversible de génération de clé (voir figure 4). Elle fait intervenir d'autres données associées au dispositif ou à la transaction, ou fournies par un compteur de remplacement de clé.

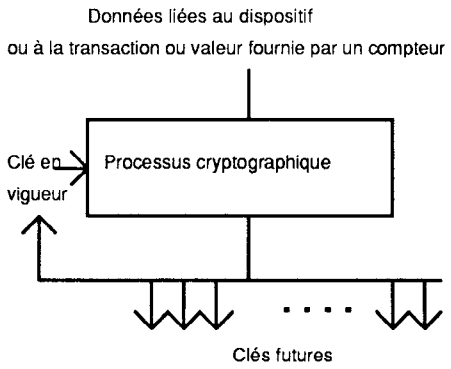

Figure 4 — Génération des clés futures

Le caractère non réversible du processus garantit que la compromission d'un dispositif cryptographique utilisant des clés transformées ne permet pas de découvrir les clés précédemment utilisées par ce dispositif, et ceci même si l'auteur de l'attaque est en possession de toutes les données en rapport avec la transformation qui ont pu exister à l'extérieur du dispositif ou d'un dispositif physiquement sûr. Les équipements en communication cryptographique avec des dispositifs qui utilisent la transformation de clé identifient à tout moment la clé utilisée

a) soit en répliquant le processus de transformation de clé en synchronisation avec le dispositif, et en stockant les clés obtenues pour un usage ultérieur,

b) soit en recevant la valeur courante du compteur de remplacement de clé, qui est inclus dans les données de la transaction reçue du dispositif, puis en générant la clé courante à partir de ce compteur et de la clé initiale. Cette procédure implique de faire toutes les transformations de clés conduisant de la clé initiale à la clé courante. En fait le nombre de transformations nécessaires reste petit (par exemple 10), même si le compteur incrémental à une valeur importante (par exemple 1 million).

5.5 Décalage de clé

Le décalage de clé permet de calculer une nouvelle clé de chiffrement de clé (KEK) à partir d'une clé initiale chaque fois qu'une nouvelle clé chiffrée doit être transmise à un nœud récepteur.

Cette technique fait obstacle à l'utilisation d'une clé antérieure (remplacée) à la place de la clé en vigueur échangée entre les deux correspondants.

La clé de chiffrement de clé initiale est combinée via un processus renouvelable (par exemple une addition modulo-2) avec un compteur incrémenté chaque fois qu'une clé de remplacement est requise. La clé obtenue est la nouvelle clé de chiffrement de clé utilisée pour chiffrer la clé de remplacement (voir figure 5).

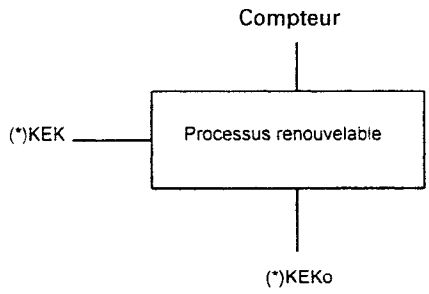

Figure 5 — Calcul d'un décalage de clé de chiffrement de clé (KEKo)

La valeur en cours du compteur est généralement transmise au nœud récepteur avec la clé chiffrée.

Le compteur a la même longueur qu'une clé, et dans le cas d'une clé double, il est combiné séparément avec les clés gauche et droite. La clé initiale sera elle-même remplacée avant la remise à zéro du compteur.

Le décalage de clé est décrit en détail dans l'ISO 8732.

5.6 Notarisation de clé

La notarisation permet d'inclure l'identité des correspondants à l'intérieur des clés de chiffrement de clé avant que le chiffrement de clé n'ait lieu.

Cette technique empêche la substitution de clé. Si une clé chiffrée est remplacée par une clé destinée à d'autres correspondants, le déchiffrement de la clé illicite produit un résultat non valide.

La notarisation de clé est décrite en détail dans l'ISO 8732.

5.7 Étiquetage de clé

Une clé utilisée à l'extérieur d'un dispositif cryptographique peut être associée à une étiquette qui en indique le type. La clé et son étiquette sont liées de façon à empêcher toute modification non détectable de l'étiquette.

Cette technique permet la séparation des clés. Elle est utilisée en combinaison avec le chiffrement de clé et elle permet le chiffrement de plusieurs types de clés au moyen d'une même clé de chiffrement de clé (KEK).

Une étiquette de clé est une constante unique choisie arbitrairement. Une étiquette de clé différente doit être attribuée à chaque type de clé devant être étiqueté. Lorsqu'une clé est générée dans le dispositif cryptographique sûr, elle est liée à l'étiquette appropriée au type de clé comme partie intégrante du processus de chiffrement de la clé, comme illustré à la figure 6. La clé étiquetée peut ensuite être stockée ou distribuée en dehors d'un dispositif cryptographique.

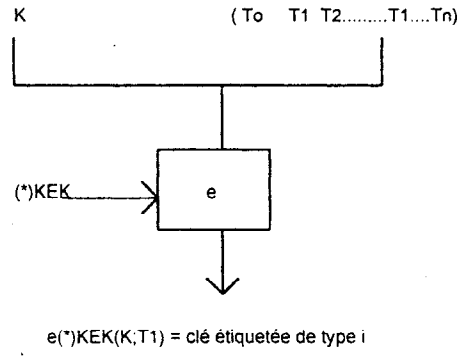

Figure 6 — Génération d'une clé étiquetée

Lorsqu'une clé étiquetée est transmise à un dispositif cryptographique sûr pour être utilisée par une fonction particulière, elle est déchiffrée, et son étiquette est reconstituée puis analysée par le dispositif (voir figure 7). Si la vérification montre que le type de la clé ne correspond pas à la valeur attendue, l'exécution de la fonction est interrompue.

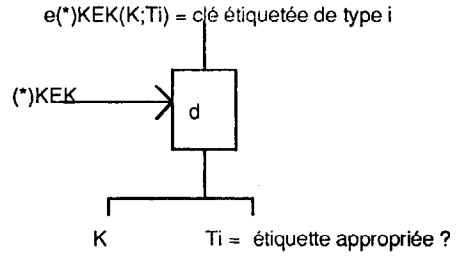

Figure 7 — Utilisation d'une clé étiquetée

Les techniques utilisées pour associer une étiquette à une clé varient selon que la longueur combinée de l'étiquette et de la clé dépasse ou non la longueur de bloc de l'algorithme cryptographique utilisé pour le chiffrement de clé. Si ce n'est pas le cas, les bits de la clé et de l'étiquette sont concaténés ou imbriqués, et le bloc résultant est chiffré. Dans le cas contraire, la clé et l'étiquette sont chiffrées comme des blocs distincts. Dans ce cas, un mode de chiffrement par chaînage (voir ISO 10116) est alors utilisé pour les associer.