NORME INTERNATIONALE

ISO 9564-1

Première édition
1991-12-15

Banque — Gestion et sécurité du numéro personnel d'identification —

Partie 1: Principes et techniques de protection du PIN

Banking — Personal Identification Number management and security —

Part 1: PIN protection principles and techniques

Numéro de référence
ISO 9564-1:1991(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 9564-1 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 9564 comprend les parties suivantes, présentées sous le titre général *Banque — Gestion et sécurité du numéro personnel d'identification*:

— *Partie 1: Principes et techniques de protection du PIN*

— *Partie 2: Algorithme(s) approuvé(s) pour le chiffrement du PIN*

Les annexes A et B font partie intégrante de la présente partie de l'ISO 9564. Les annexes C, D, E, F, G et H sont données uniquement à titre d'information.

Introduction

Le numéro d'identification personnel (PIN) est un moyen de vérifier l'identité d'un client dans un système de transfert électronique de fonds (EFT).

La gestion du PIN a pour but de protéger le PIN contre toute divulgation non autorisée, contre sa découverte et sa mauvaise utilisation au cours de sa durée de vie et, ce faisant, minimiser les risques de fraude survenant dans les systèmes EFT. Le secret du PIN doit être assuré à tout moment au cours de sa durée de vie qui comprend sa sélection, son émission, son activation, sa mise en mémoire, sa saisie, sa transmission, sa validation, sa désactivation et tout autre emploi pouvant en être fait.

La sécurité du PIN dépend également d'une gestion de clés saine. Sauvegarder le secret des clés de chiffrement est primordial car la découverte de n'importe quelle clé compromet tout PIN précédemment chiffré par cette clé.

Dans la mesure du possible, la présente partie de l'ISO 9564 spécifie des exigences en termes absolus. Dans certains cas, il n'est pratiquement pas possible d'éviter un certain niveau de subjectivité surtout lorsqu'il s'agit du degré de niveau de sécurité souhaité ou à atteindre.

Le niveau de sécurité à atteindre doit intégrer un certain nombre de facteurs, y compris la sensibilité des données concernées et l'éventualité de leur interception, la possibilité pratique de tout procédé de chiffrement envisagé et le coût de l'obtention et de la violation d'un système particulier de sécurité. Par conséquent, il est nécessaire que l'accepteur, l'acquéreur et l'émetteur de carte s'accordent sur l'étendue et le détail des procédures de sécurité et de gestion du PIN. Il n'est pratiquement pas possible d'atteindre une sécurité absolue; c'est pourquoi les procédures de gestion du PIN ne devraient pas uniquement viser à réduire la possibilité d'une violation de sécurité mais devraient également viser à détecter avec une très forte probabilité tout accès illicite ou changement du matériel du PIN susceptible d'advenir en dépit des mesures préventives. Ceci s'applique à toutes les étapes de la génération, de l'échange et de l'utilisation d'un PIN, notamment les procédés intervenant dans l'équipement de chiffrement et ceux liés à la communication des PIN.

La présente partie de l'ISO 9564 est conçue de façon que les émetteurs puissent s'assurer uniformément, au degré le plus pratique possible, qu'un PIN, tout en étant sous le contrôle d'autres institutions, est correctement géré. Des techniques sont données pour protéger le processus d'authentification du client basé sur le PIN en sauvegardant le PIN contre une divulgation non autorisée au cours de son cycle de vie.

La présente partie de l'ISO 9564 présente des techniques de protection du PIN contre toute divulgation non autorisée au cours de sa durée de vie et comprend les annexes suivantes:

a) l'annexe A donne les procédures d'approbation d'un algorithme de chiffrement;

b) l'annexe B traite des principes généraux de gestion de clé;

c) l'annexe C traite des techniques de vérification du PIN;

d) l'annexe D traite des concepts de mise en œuvre d'un dispositif de saisie du PIN;

e) l'annexe E présente un exemple de génération de PIN pseudo-aléatoire;

f) l'annexe F donne des directives complémentaires pour la conception du clavier d'entrée du PIN;

g) l'annexe G spécifie l'abrogation des supports d'enregistrement utilisés pour le stockage des éléments de mise à la clé;

h) l'annexe H donne des informations destinées aux clients.

Dans l'ISO 9564-2 sont spécifiés les algorithmes approuvés de chiffrement qui doivent être utilisés pour la protection du PIN. L'application des exigences de la présente partie de l'ISO 9564 requiert la conclusion d'accords bilatéraux, y compris ce qui concerne le choix des algorithmes spécifiés dans l'ISO 9564-2.

La présente partie de l'ISO 9564 fait partie d'une série de normes décrivant les prescriptions de sécurité dans l'environnement bancaire, comme suit:

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

ISO 9564-2:1991, *Banque — Gestion et sécurité du numéro personnel d'identification — Partie 2: Algorithme(s) approuvé(s) pour le chiffrement du PIN.*

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

Les prescriptions de l'ISO 9564 sont compatibles avec celles de l'ISO 8583 en ce qui concerne la sécurité des informations connexes.

Banque — Gestion et sécurité du numéro personnel d'identification —

Partie 1:
Principes et techniques de protection du PIN

1 Domaine d'application

La présente partie de l'ISO 9564 prescrit les mesures de sécurité minimales nécessaires à une gestion efficace du PIN. Des mesures normalisées permettant d'échanger des informations liées au PIN sont indiquées. La présente partie de l'ISO 9564 prescrit également les règles liées à l'approbation des algorithmes de chiffrement du PIN. La présente partie de l'ISO 9564 s'applique aux institutions responsables des techniques de mise en œuvre de gestion et de protection du PIN liées aux transactions initiées par carte bancaire. Les dispositions de la présente partie de l'ISO 9564 ne couvrent pas

— la protection du PIN contre la perte ou la mauvaise utilisation volontaire par le client ou les employés de l'émetteur;

— la protection de données d'une transaction non protégées par un PIN;

— la protection de messages de transaction envers leur modification ou leur substitution (par exemple une réponse d'autorisation à une vérification de PIN);

— la protection contre la répétition du PIN ou de la transaction;

— les techniques spécifiques de gestion de clés;

— la gestion du PIN et la sécurité des transactions réalisées au moyen des cartes à circuit intégré (ICC);

— l'utilisation d'algorithmes de chiffrement asymétriques pour la gestion du PIN.

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 9564. 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 9564 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 7812:1987, *Cartes d'identification — Système de numérotation et procédure d'enregistrement pour les identificateurs d'émetteur.*

ISO 8583:1987, *Messages initiés par carte bancaire — Spécifications d'échange de messages — Contenu pour les transactions financières.*

ISO 8908:—[1], *Banque et services financiers liés aux opérations bancaires — Vocabulaire et éléments de données.*

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

American National Standard X3.92:1981, *Data Encryption Algorithm (DEA).*

3 Définitions

Pour les besoins de la présente partie de l'ISO 9564, les définitions suivantes s'appliquent.

3.1 acquéreur: Institution (ou son agent) qui acquiert de l'accepteur de la carte l'information financière liée à la transaction et introduit cette information dans un système d'interchange.

3.2 algorithme: Processus mathématique défini sans ambiguïté.

3.3 accepteur de carte: Partie acceptant la carte et présentant les données de la transaction à un acquéreur.

3.4 texte chiffré: Information dans sa forme chiffrée.

3.5 découverte: En chiffrement, la violation du secret et/ou de la sécurité.

3.6 clé de chiffrement: Valeur mathématique utilisée dans un algorithme pour transformer un texte en clair en texte chiffré ou vice versa.

3.7 client: Individu associé au numéro de compte primaire (PAN) spécifié dans la transaction.

3.8 déchiffrement: Transformation inverse d'un chiffrement réversible préalable; action permettant de rendre un texte chiffré intelligible.

3.9 double contrôle: Intervention de deux entités distinctes ou plus (généralement des personnes) opérant de concert pour protéger des fonctions ou des informations sensibles, aucun individu isolé ne pouvant accéder aux éléments ni les utiliser, par exemple une clé de chiffrement.

3.10 chiffrement: Action permettant de rendre un texte inintelligible au moyen d'un mécanisme de codage.

3.11 chiffrement irréversible: Transformation d'un texte en clair en texte chiffré de telle façon que le texte en clair original ne puisse pas être retrouvé autrement qu'avec des procédures exhaustives même si la clé de chiffrement est connue.

3.12 transformation irréversible d'une clé: Nouvelle clé générée à partir d'une clé préalable de telle sorte qu'il n'existe pas de technique permettant de déterminer l'ancienne clé même en connaissant la nouvelle clé et tous les détails de la transformation.

3.13 émetteur: Institution tenant le compte identifié par le numéro de compte primaire (PAN).

3.14 élément de clé: Un parmi au moins deux paramètres possédant le format d'une clé cryptographique, qui est additionné modulo-2 à un ou plusieurs paramètres semblables pour former une clé de chiffrement.

3.15 addition modulo-2: Addition binaire sans retenue (appelée également ou-exclusif).

3.16 nœud: Toute entité de traitement de message par laquelle passe une transaction.

---

1) À publier.

3.17 notarisation: Méthode permettant de modifier une clé de chiffrement de clé dans le but d'authentifier l'identité de l'expéditeur et du destinataire final.

3.18 numéro d'identification personnel (PIN): Code ou mot de passe possédé par le client pour la vérification de son identité.

3.19 texte en clair: Données dans leur forme originale non chiffrée.

3.20 numéro de compte primaire (PAN): Numéro attribué qui identifie l'émetteur et le porteur de la carte. Ce numéro est composé d'un numéro d'identification de l'émetteur, de l'identification du numéro de compte individuel et d'un chiffre de vérification associé, comme le définit l'ISO 7812.

3.21 nombre pseudo-aléatoire: Nombre statistiquement aléatoire et essentiellement imprévisible bien que généré par un procédé algorithmique.

3.22 PIN de référence: Valeur du PIN utilisée pour vérifier le PIN de transaction.

3.23 chiffrement réversible: Transformation d'un texte en clair en texte chiffré de telle sorte que le texte en clair original puisse être retrouvé.

3.24 connaissance répartie: Contexte dans lequel au moins deux entités se partagent en les gardant secrets les éléments d'une clé unique qui, pris isolément, ne permettent pas de déduire la clé de chiffrement résultant de leur combinaison.

3.25 PIN de transaction: Terme utilisé pour décrire le PIN tel qu'il est saisi par le client.

3.26 variante d'une clé: Nouvelle clé formée par un procédé non secret à partir de la clé originale, de telle sorte qu'un ou plusieurs bits de la nouvelle clé, à l'exclusion des bits de parité, soient différents des bits correspondants de la clé originale.

4 Principes de base de gestion du PIN

La gestion du PIN doit être régie par les principes de base suivants:

a) Pour toutes les fonctions de gestion du PIN, des contrôles doivent être appliqués de sorte que le matériel et le logiciel utilisés ne puissent pas être modifiés de façon frauduleuse ou qu'on ne puisse y avoir accès sans enregistrement, détection et/ou invalidation comme indiqué en 6.1.1.

b) Après la sélection, le PIN, s'il est mémorisé, doit être chiffré lorsqu'il ne peut pas être mécaniquement sauvegardé, comme indiqué en 6.2 et 7.7.

c) Pour différents comptes, le chiffrement de la même valeur de PIN sous une clé de chiffrement donnée ne doit pas produire de façon prévisible le même texte chiffré comme indiqué en 6.2.

d) La sécurité d'un PIN chiffré ne doit pas reposer sur la confidentialité de la conception ou de l'algorithme de chiffrement mais sur une clé secrète comme indiqué en 6.2.

e) Le PIN en texte clair ne doit jamais se trouver dans les locaux de l'acquéreur sauf s'il est placé à l'intérieur d'un dispositif physiquement sûr comme indiqué en 6.3.1.

f) Un PIN en texte clair peut se trouver dans les locaux contenant l'ordinateur de l'émetteur, à condition que ces locaux constituent un environnement physiquement sûr au cours de la période définie en 6.3.2.

g) Seul le client et/ou le personnel autorisé par l'émetteur doivent être impliqués dans la sélection du PIN (voir 7.2), l'émission du PIN ou tout procédé de saisie du PIN dans lequel le PIN peut être lié à des informations d'identité du compte. Ce personnel doit opérer en respectant strictement les procédures prescrites (par exemple double contrôle).

h) Un PIN chiffré stocké doit être protégé contre la substitution, comme indiqué en 7.7.

i) La découverte d'un PIN (ou une menace de découverte) doit se traduire par la fin de la durée de vie du PIN comme indiqué en 7.8.

j) L'émetteur est responsable de la vérification du PIN, bien que la fonction de vérification puisse être déléguée à une autre institution comme indiqué en 8.5.

k) Des clés de chiffrement différentes doivent être utilisées pour la protection du stockage du PIN et de la transmission comme indiqué en 6.2.

l) Le client doit être informé par écrit de l'importance du PIN et de sa confidentialité (voir annexe H).

5 Claviers d'entrée du PIN

5.1 Jeu de caractères

Tous les claviers d'entrée du PIN doivent permettre la saisie des caractères numériques décimaux de 0 (zéro) à 9 (neuf).

NOTE 1 Il est reconnu que les caractères alphabétiques, bien que non attribués dans la présente partie de l'ISO 9564, peuvent être utilisés comme synonymes des caractères numériques décimaux. De plus amples informations sur la conception des claviers d'entrée du PIN, comprenant les correspondances entre caractères alphabétiques et numériques, sont données dans l'annexe F.

5.2 Représentation des caractères

La relation entre la valeur numérique d'un caractère du PIN et le codage interne de cette valeur avant tout chiffrement doit être comme indiqué dans le tableau 1.

Tableau 1 — Représentation des caractères

Caractère du PIN	Binaire interne
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

5.3 Saisie du PIN

Les valeurs du PIN saisi ne doivent pas être affichées en clair ni divulguées par signal sonore.

5.4 Éléments à prendre en compte pour la présentation physique

Un clavier d'entrée du PIN peut physiquement se présenter comme partie intégrante d'un terminal, ou peut se trouver éloigné de l'électronique de gestion du terminal. L'électronique de gestion du terminal peut être ou non protégée physiquement (voir définition en 6.3.1); quoiqu'il en soit, le clavier d'entrée du PIN doit être protégé comme indiqué en 6.3.1 ou en 6.3.3.

Le clavier d'entrée du PIN doit être conçu et installé de sorte que le client puisse empêcher des tiers d'observer la valeur du PIN au moment de sa saisie.

Lorsqu'on utilise un clavier d'entrée du PIN éloigné, la liaison physique entre celui-ci et le terminal associé doit être protégée (voir 8.2).

Le tableau 2 résume les prescriptions de sécurité pour chacune des quatre configurations possibles pour le terminal et le clavier d'entrée du PIN.

Tableau 2 — Éléments à prendre en compte pour la présentation physique du clavier

	Terminal protégé physiquement	Terminal non protégé physiquement
Clavier d'entrée du PIN intégré au terminal	Les exigences de protection physique comme indiqué en 6.3.1 s'appliquent à tout le terminal. Le terminal doit chiffrer le PIN comme indiqué en 6.2, avant sa transmission.	Les exigences de protection physique comme indiqué en 6.3.1 ou en 6.3.3 s'appliquent au clavier d'entrée du PIN. Le clavier d'entrée du PIN doit chiffrer le PIN comme indiqué en 6.2, avant sa transmission.
Clavier d'entrée du PIN éloigné du terminal	Le clavier d'entrée du PIN doit être protégé comme spécifié en 6.3.1 ou en 6.3.3. Le clavier d'entrée du PIN doit chiffrer le PIN comme indiqué en 6.2, avant sa transmission.	Le clavier d'entrée du PIN doit être protégé comme indiqué en 6.3.1 ou en 6.3.3. Le clavier d'entrée du PIN doit chiffrer le PIN comme indiqué en 6.2, avant sa transmission.

6 Problèmes liés à la sécurité du PIN

6.1 Procédures de contrôle du PIN

6.1.1 Matériel et logiciel

Le matériel et le logiciel utilisés pour les fonctions de gestion du PIN doivent être mis en œuvre de façon à garantir les points suivants.

a) Le matériel et le logiciel assurent correctement la fonction pour laquelle ils ont été conçus et uniquement cette fonction.

b) Aucune modification ni accès au matériel et au logiciel ne peut survenir sans détection et/ou invalidation.

c) Aucune modification ni accès frauduleux aux informations ne peut survenir sans détection et/ou invalidation.

d) Le système ne doit pas pouvoir être utilisé ou mal utilisé dans le but de rechercher un PIN par essai réitéré des PINS erronés.

NOTE 2 Des listages imprimés ou sur microfilm ou les image-mémoires utilisés pour la sélection, le calcul ou le chiffrement du PIN devraient être contrôlés en cours d'utilisation, de livraison, de stockage et de destruction.

6.1.2 Supports d'enregistrements

Tous les supports d'enregistrement (par exemple bande magnétique, disques) contenant des informations à partir desquelles un PIN en clair peut être déterminé, doivent être démagnétisés, écrasés, ou détruits physiquement immédiatement après leur utilisation. Un système informatique ne pourra être utilisé, pour ce faire,

que si toutes les zones de mémoire (y compris de mémorisation temporaire) utilisées dans le processus ci-dessus peuvent être spécifiquement identifiées et démagnétisées ou écrasées (voir annexe G).

6.1.3 Communications orales

Aucune procédure ne doit nécessiter ou permettre la communication orale du PIN en clair, par téléphone ou en personne. Une institution ne doit jamais autoriser ses employés à demander à un client de divulguer le PIN ou à recommander des valeurs spécifiques.

6.1.4 Claviers téléphoniques

Les procédures d'une institution ne doivent pas autoriser la saisie du PIN en clair par l'intermédiaire de touches téléphoniques, sauf si le combiné téléphonique est conçu et réalisé pour répondre aux exigences de 5.4 pour les claviers d'entrée du PIN et de 8.2 pour la transmission du PIN.

6.2 Chiffrement du PIN

Lorsqu'il est nécessaire de chiffrer un PIN pour sa mise en mémoire et sa transmission (voir 6.3 et 8.2), cela doit être effectué en utilisant l'un des algorithmes approuvés spécifiés dans l'ISO 9564-2.

La procédure de chiffrement adoptée doit garantir que le chiffrement d'une valeur de PIN en clair utilisant une clé de chiffrement particulière ne produit pas de façon prévisible la même valeur chiffrée lorsque la même valeur du PIN est associée à différents comptes (voir 7.8).

Des clés de chiffrement différentes doivent être utilisées pour protéger le PIN de référence et le PIN de transaction.

Les clés de chiffrement du PIN ne doivent pas être utilisées à d'autres fins cryptographiques.

Voir annexe B pour les principes généraux de gestion de clé.

6.3 Sécurité physique

Ce paragraphe définit un «dispositif physiquement sûr» et un «environnement physiquement sûr» et spécifie les prescriptions relatives à un appareil de saisie du PIN.

Un PIN de référence non chiffré ne doit exister que dans «un environnement physiquement sûr» ou dans un «dispositif physiquement sûr». Un PIN de transaction non chiffré ne doit exister que dans «un dispositif physiquement sûr», un appareil de saisie du PIN satisfaisant aux prescriptions de 6.3.3 ou dans «l'environnement physiquement sûr» de l'émetteur (ou de l'agent de l'émetteur).

6.3.1 Dispositif physiquement sûr

Pour évaluer la sécurité physique de tout dispositif, on doit prendre en considération l'environnement opérationnel dans lequel celui-ci est mis en œuvre. Un dispositif physiquement sûr est un dispositif physique dans lequel lorsqu'il est mis en œuvre d'une manière et dans un environnement adéquats on ne peut s'introduire pour ensuite pouvoir divulguer tout ou partie de clé cryptographique ou de PIN résidant dans le dispositif.

L'entrée dans le dispositif quand il est mis en œuvre dans un environnement et d'une manière adéquate doit provoquer l'effacement automatique et immédiat de tous les PINs, clés de chiffrement et tous les restes de PIN utiles et de clés contenus dans le dispositif.

Un dispositif ne doit être utilisé comme un dispositif physiquement sûr que lorsqu'on est sûr que le fonctionnement interne de celui-ci n'a pas été modifié dans le but d'en permettre l'intrusion (par exemple insertion dans le dispositif d'un mécanisme actif ou passif d'écoute clandestine).