NORME INTERNATIONALE

ISO 13491-1

Première édition
1998-06-15

Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) —

Partie 1:
Concepts, prescriptions et méthodes d'évaluation

Banking — Secure cryptographic devices (retail) —
Part 1: Concepts, requirements and evaluation methods

Numéro de référence
ISO 13491-1:1998(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 Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 3.

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 13491-1 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 13491 comprend les parties suivantes, présentées sous le titre général *Banque — Dispositifs cryptographiques de sécurité (services aux particuliers)*:

— *Partie 1: Concepts, prescriptions et méthodes d'évaluation*

— *Partie 2: Listes de contrôle de la conformité à la sécurité pour les dispositifs utilisés dans les systèmes de cartes à bande magnétique*

L'annexe A de la présente partie de l'ISO 13491 est donnée uniquement à titre d'information.

Introduction

L'ISO 13491 décrit à la fois les caractéristiques physiques et logiques et la gestion des dispositifs cryptographiques de sécurité (SCD) employés pour protéger les messages, les clés cryptographiques et les autres informations sensibles utilisées dans le cadre des services bancaires aux particuliers, où un SCD est un dispositif matériel protégé physiquement et logiquement assurant un ensemble de services cryptographiques de sécurité.

La sécurité des services bancaires électroniques aux particuliers dépend largement de la sécurité de ces dispositifs cryptographiques. Cette sécurité est basée sur le principe selon lequel l'accès et la manipulation des fichiers informatiques sont possibles, les lignes de communication peuvent faire l'objet d'une écoute clandestine, et que des données autorisées ou des saisies de commandes dans l'équipement du système peuvent être remplacées par des saisies non autorisées. Si certains équipements cryptographiques (par exemple, les modules de sécurité d'hôte) restent concentrés à l'intérieur de centres de traitement dont la sécurité est relativement élevée, une large proportion de dispositifs cryptographiques utilisés dans les services bancaires aux particuliers (par exemple, les claviers de saisie de PIN, les guichets automatiques bancaires, etc.) sont installés dans des environnements non sécurisés. Par conséquent, lorsque des Numéros personnels d'identification (PIN), des Codes d'authentification de message (MAC), des clés cryptographiques et autres données sensibles, sont traités dans ces dispositifs, il existe un risque que ces derniers soient attaqués ou compromis de manière à divulguer ou à modifier ces données. On doit donc réduire le risque financier par l'utilisation appropriée de dispositifs cryptographiques dotés des caractéristiques adéquates et gérés correctement.

Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) —

Partie 1:
Concepts, prescriptions et méthodes d'évaluation

1 Domaine d'application

La présente partie de l'ISO 13491 spécifie les prescriptions concernant les Dispositifs Cryptographiques de Sécurité qui intègrent les procédés cryptographiques définis dans l'ISO 9564, l'ISO 9807 et l'ISO 11568.

La présente partie de l'ISO 13491 vise deux principaux objectifs:

1. établir les prescriptions concernant les caractéristiques opérationnelles des SCD et la gestion de ces dispositifs à travers les diverses étapes de leur cycle de vie;
2. normaliser la méthodologie de vérification de la conformité aux prescriptions en question.

Il est nécessaire que ces dispositifs soient dotés de caractéristiques garantissant qu'ils disposent des capacités opérationnelles adéquates et qu'ils assurent la protection qui convient aux données qu'ils contiennent. Une bonne gestion de ces dispositifs est nécessaire pour garantir que le dispositif considéré est légitime, qu'il n'a pas été modifié de manière illicite, par exemple par «bogage», et que les données sensibles qu'il peut contenir (par exemple, des clés cryptographiques) n'ont été ni divulguées ni modifiées.

D'un point de vue pratique, il est impossible de garantir une sécurité absolue. La sécurité cryptographique dépend de chaque phase du cycle de vie du SCD et de la combinaison complémentaire des procédures de gestion appropriées et des caractéristiques cryptographiques sécurisées. Ces procédures de gestion mettent en œuvre des mesures préventives pour réduire l'opportunité d'une violation de la sécurité du dispositif cryptographique. Elles ont pour but un haut niveau de probabilité de détection des accès illicites aux données sensibles ou confidentielles dans le cas où les caractéristiques des dispositifs ne parviendraient pas à empêcher ou à détecter la compromission de sécurité.

L'annexe A contient une illustration informative des concepts de niveaux de sécurité décrits dans la présente partie de l'ISO 13491 applicables aux dispositifs cryptographiques de sécurité.

La présente partie de l'ISO 13491 ne traite pas les questions liées au refus de service d'un SCD.

Les prescriptions spécifiques concernant les caractéristiques et la gestion des types spécifiques de fonctionnalités des SCD utilisées dans le cadre des services bancaires aux particuliers sont décrites dans une autre partie de l'ISO 13491.

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 13491. 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 13491 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 7498-2:1989, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Partie 2: Architecture de sécurité.*

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

ISO 9564-1:—[1)], *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 10202 (toutes les parties), *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré.*

ISO 11568 (toutes les parties), *Banque — Gestion de clés (services aux particuliers).*

ISO 13491-2:—[2)], *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 Termes et définitions

Pour les besoins de la présente partie de l'ISO 13491, les termes et définitions données dans l'ISO 8908, ainsi que les suivants, s'appliquent.

3.1
autorité d'accréditation
autorité responsable de l'accréditation des autorités d'évaluation et de la supervision de leur travail de manière à garantir la reproductibilité des résultats des évaluations

3.2
autorité d'évaluation accréditée
organisme accrédité conformément à un ensemble de règles, par exemple EN 45000 ou le Guide ISO 25, et accepté par l'autorité d'accréditation aux fins de l'évaluation

3.3
attaque
tentative par un adversaire sur le dispositif en vue d'obtenir ou de modifier des informations sensibles ou un service qu'il n'est pas autorisé à obtenir ou à modifier

3.4
liste de contrôle d'audit
liste de prescriptions à contrôler, organisée par type de dispositif, et contenue dans une autre partie de l'ISO 13491

3.5
compte rendu d'audit
document émis par l'Organisme d'examen d'audit basé sur les résultats obtenus par un auditeur

3.6
organisme d'examen d'audit
groupe ayant la responsabilité d'examiner et de juger les résultats obtenus par l'auditeur

---

1) À publier. (Révision de l'ISO 9564-1:1991)

2) À publier.

3.7
auditeur
personne chargée de vérifier, d'estimer, d'examiner et d'évaluer la conformité à une évaluation informelle au nom du commanditaire ou de l'Organisme d'examen d'audit

3.8
compte rendu de certification
document produit par l'organisme d'examen d'évaluation sur la base des résultats obtenus auprès d'une autorité d'évaluation accréditée

3.9
contrôleur
entité responsable de la gestion sûre d'un SCD

3.10
livraison
documents, équipement et autres articles ou informations nécessaires aux personnes chargées de l'évaluation pour réaliser une évaluation du Dispositif Cryptographique de Sécurité

3.11
sécurité d'un dispositif
sécurité du SCD compte tenu de ses caractéristiques uniquement, sans référence à un environnement opérationnel particulier

3.12
sécurité dépendante de l'environnement
sécurité d'un SCD dans le cadre d'un environnement opérationnel

3.13
agence d'évaluation
organisme bénéficiant de la confiance des autorités de conception, de fabrication et commanditaire, chargée d'évaluer le SDC (au moyen de compétences et d'outils spécialisés) conformément à la présente partie de l'ISO 13491

3.14
compte rendu d'évaluation
document émis par l'organisme d'examen d'évaluation sur la base des résultats obtenus auprès d'une agence d'évaluation ou d'un auditeur

3.15
organisme d'examen d'évaluation
groupe chargé d'examiner et de juger les résultats de l'agence d'évaluation

3.16
prescriptions formelles
déclarations concernant les caractéristiques et fonctions d'un Dispositif Cryptographique de Sécurité

3.17
sécurité logique
capacité d'un dispositif à résister aux attaques à travers son interface fonctionnelle

3.18
environnement opérationnel
environnement dans lequel le SCD est exploité, c'est-à-dire le système d'application dont il fait partie, son emplacement, les personnes qui l'exploitent et l'utilisent et les entités qui communiquent avec lui

3.19
sécurité physique
capacité d'un dispositif à résister aux attaques contre sa construction physique

3.20
dispositif cryptographique de sécurité; SCD
dispositif matériel protégé physiquement et logiquement, qui assure un ensemble sécurisé de services cryptographiques

3.21
interface du SCD
interface du SCD par l'intermédiaire de laquelle le SCD interagit avec l'environnement opérationnel (par exemple, les commandes, les panneaux de contrôle, le verrouillage, etc.)

3.22
données sensibles; informations sensibles
données, caractéristiques de conception, informations d'état, clés cryptographiques, etc. qui doivent être protégées contre la divulgation non autorisée, l'altération et la destruction

3.23
logiciel
programmes et/ou données qui seront utilisés par le SCD ou téléchargés pour être utilisés par le SCD

3.24
autorité commanditaire; commanditaire
personne, entreprise ou organisme exigeant l'évaluation du SCD

3.25
caractéristique de preuve d'attaque
caractéristique qui fournit la preuve qu'une attaque a été tentée

3.26
caractéristique de résistance aux attaques
caractéristique qui assure la protection physique passive contre une attaque

3.27
caractéristique de réponse aux attaques
caractéristique qui assure une réponse active à la détection d'une attaque, de manière à l'empêcher de réussir

4 Concepts de dispositifs cryptographiques de sécurité

Les dispositifs cryptographiques sont utilisés dans le cadre des services bancaires aux particuliers pour assurer

— l'intégrité des données sensibles, par exemple les détails d'une transaction;

— la confidentialité des informations secrètes, par exemple les codes PIN des clients;

— la confidentialité des clés cryptographiques utilisées pour atteindre ces objectifs.

Pour remplir les obligations ci-dessus, les dangers ci-dessous doivent être contrés:

— divulgation d'informations sensibles stockées ou saisies dans le dispositif;

— modification d'informations sensibles;

— utilisation non autorisée d'un dispositif;

— accès non autorisé à un service.

La sécurité absolue étant impossible à atteindre, il n'est pas réaliste de décrire un SCD comme étant «100 % inviolable» ou «physiquement sûr». Moyennant l'investissement, les efforts et les compétences nécessaires, il sera toujours possible de surmonter un schéma de sécurité. Qui plus est, avec les progrès de la technologie, de nouvelles techniques seront développées pour attaquer un schéma de sécurité jusque là réputé résistant aux

attaques. De ce fait, il est plus réaliste de caractériser un dispositif de sécurité comme possédant un degré de résistance à l'attaque, un degré acceptable correspondant à la capacité d'empêcher toute attaque envisageable pendant la vie opérationnelle du dispositif, en tenant compte de l'équipement, du savoir-faire et des autres frais qu'un adversaire devrait engager pour monter une attaque réussie, ainsi que du profit financier que l'adversaire en question pourrait tirer de pareille attaque.

La sécurité des systèmes de services aux particuliers considère les aspects physiques et logiques de la sécurité des dispositifs, la sécurité de l'environnement opérationnel et la gestion du dispositif. Ces facteurs établissent conjointement la sécurité des dispositifs et celle des applications qui les utilisent. Les besoins de sécurité sont déduits de l'évaluation des risques liés aux applications prévues.

Les caractéristiques de sécurité requises vont dépendre de l'application prévue et de l'environnement opérationnel, ainsi que des types d'attaques à considérer. Une évaluation des risques devrait être réalisée pour permettre de sélectionner la méthode la mieux appropriée pour estimer la sécurité du dispositif. Les résultats sont ensuite évalués de manière à accepter les dispositifs pour une application et un environnement donnés. Les méthodes normalisées d'évaluation sont énumérées dans l'article 7.

4.1 Scénarios d'attaque

Les scénarios d'attaque décrits ne constituent pas une liste exhaustive, mais sont indicatifs des principales zones de risque. Les SCD sont soumis à cinq grandes catégories d'attaques:

— pénétration;

— surveillance;

— manipulation;

— modification;

— substitution.

Ces attaques sont décrites ci-dessous.

4.1.1 Pénétration

La pénétration est une attaque active résultant de la perforation physique ou de l'ouverture non autorisée du dispositif pour vérifier les données sensibles qu'il contient, par exemple, des clés cryptographiques. Par conséquent, la pénétration est une attaque contre les caractéristiques physiques du dispositif.

4.1.2 Surveillance

La surveillance est une attaque passive pouvant nécessiter la surveillance des rayons électromagnétiques de manière à découvrir les informations sensibles contenues dans le dispositif; ou la surveillance visuelle, auditive ou électronique des données secrètes saisies dans le dispositif. Par conséquent, la surveillance est une attaque contre les caractéristiques physiques du dispositif.

4.1.3 Manipulation

La manipulation est l'envoi non autorisé au dispositif d'une séquence de saisies de manière à provoquer la divulgation d'informations sensibles ou obtenir un service de manière non autorisée, par exemple, faire passer le dispositif en «mode test» pour que les informations sensibles puissent être divulguées ou que l'intégrité du dispositif soit manipulée. La manipulation est une attaque contre les caractéristiques logiques du dispositif.

4.1.4 Modification

La modification est la transformation ou l'altération non autorisée des caractéristiques logiques ou physiques du dispositif, par exemple, l'introduction d'un «bogue» de divulgation de PIN sur un clavier de saisie de PIN, entre le point de saisie et le point de chiffrement du PIN. La modification peut nécessiter la pénétration; dans ce cas, le but est d'altérer le dispositif et non pas de divulguer les données qu'il contient. Le remplacement non autorisé d'une clé

cryptographique contenue dans un dispositif est une forme de modification. La modification est une attaque contre les caractéristiques physiques ou logiques d'un dispositif.

4.1.5 Substitution

La substitution est le remplacement non autorisé d'un dispositif par un autre. Le dispositif de remplacement peut ressembler à une «contrefaçon» ou à une émulation du dispositif considéré, doté de toutes ou de certaines des ses caractéristiques logiques et de fonctions non autorisées, par exemple un bogue de divulgation de PIN. Le dispositif de remplacement peut être un ancien dispositif légitime soumis à des modifications non autorisées puis substitué à un autre dispositif légitime. Le retrait est une forme de substitution qui peut être effectuée pour réaliser une attaque par pénétration ou par modification dans un environnement mieux adapté pour ce type d'attaque ou, à titre de première étape dans une attaque par substitution, le dispositif peut être retiré de son environnement de fonctionnement. La substitution peut être considérée comme un cas particulier de modification dans lequel l'adversaire ne modifie pas le dispositif cible, mais le remplace par un substitut modifié. La substitution est une attaque contre les caractéristiques physiques et logiques du dispositif.

4.2 Mesures défensives

Pour assurer la défense contre les scénarios d'attaque décrits ci-dessus, trois facteurs contribuent au niveau de sécurité requis:

— les caractéristiques du dispositif;

— la gestion du dispositif;

— l'environnement.

Si dans certains cas un seul facteur, par exemple les caractéristiques du dispositif, peut être prédominant, en général, tous les facteurs sont nécessaires pour assurer le résultat souhaité.

4.2.1 Caractéristiques des dispositifs

Les dispositifs cryptographiques sont conçus et mis en œuvre avec une sécurité logique et physique de manière à empêcher les scénarios d'attaque décrits en 4.1, comme l'indiquent les résultats de l'évaluation des risques de l'application et de l'environnement.

Le but principal des caractéristiques physiques d'un dispositif de sécurité est d'assurer la défense contre les attaques par pénétration. Ces caractéristiques peuvent être réparties en trois catégories:

— caractéristiques de preuve d'attaque;

— caractéristiques de résistance aux attaques;

— caractéristiques de réponse aux attaques.

Le but de la preuve d'attaque est de prouver qu'une attaque a été tentée et peut avoir ou ne pas avoir entraîné la divulgation, l'utilisation ou la modification non autorisée des informations sensibles. La découverte d'une tentative d'attaque peut prendre la forme d'une preuve physique, par exemple la détérioration du conditionnement, ou l'absence du dispositif de son emplacement prévu.

Le but de la résistance aux attaques est de bloquer les attaques contre les informations à protéger contre la divulgation, l'utilisation ou la modification non autorisée, au moyen de barrières passives. Les défenses ou blocages ont généralement un but unique, à savoir qu'ils sont conçus pour bloquer un danger spécifique. La mise en œuvre de conceptions résistantes aux attaques dépend énormément des connaissances du concepteur et de l'expérience d'attaques antérieures contre une conception spécifique. C'est pourquoi les attaques contre les conceptions résistantes aux attaques visent généralement à découvrir, parmi les dangers connus, celui que le concepteur n'a pas prévu. L'attaquant va également tenter de découvrir de nouvelles attaques susceptibles d'être inconnues du concepteur. L'évaluation d'une conception résistante aux attaques est difficile et peu concluante, car elle se contente généralement de démontrer que la conception parvient à bloquer les attaques connues pour lesquelles elle a été prévue, mais n'évalue pas, ou ne parvient pas à évaluer, la résistance aux attaques inconnues.