NORME INTERNATIONALE

ISO 9807

Première édition
1991-12-15

Banque et services financiers liés aux opérations bancaires — Spécifications liées à l'authentification des messages (service aux particuliers)

Banking and related financial services — Requirements for message authentication (retail)

Numéro de référence
ISO 9807:1991(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 9807 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, B et C font partie intégrante de la présente Norme internationale. Les annexes D, E, F et G sont données uniquement à titre d'information.

Introduction

Un code d'authentification de message [(MAC) — «Message Authentication Code»] peut être utilisé pour authentifier l'origine et le texte d'un message échangé entre un expéditeur et un destinataire. Il est généré par l'expéditeur du message et est transmis en même temps que le message auquel il se rapporte.

La présente Norme internationale a été élaborée pour que les institutions offrant des services bancaires aux particuliers (retail) et souhaitant mettre en place un système d'authentification des messages puissent le faire en toute sécurité, d'une manière qui facilite l'interopérabilité entre des systèmes différents.

Un code d'authentification de message (MAC) est une zone de données qui peut être utilisée pour vérifier l'authenticité d'un message. Il est obtenu à partir du message complet ou de certains éléments de données du message qui doivent être protégés contre toute altération, que ces altérations surviennent accidentellement ou soient le fait d'une action frauduleuse.

La présente Norme internationale fait partie d'une série qui décrit les spécifications de sécurité dans les services aux particuliers. (Voir annexe G.)

Une série de Normes internationales connexes décrit les spécifications de sécurité dans les services aux entreprises (wholesale). (Voir annexe G.)

Les prescriptions de la présente Norme internationale sont compatibles avec celles de l'ISO 8730. La présente Norme internationale ainsi que l'ISO 8730 sont étroitement liées à l'ISO 8731 qui décrit des algorithmes dont l'utilisation a été approuvée pour l'authentification des messages.

Banque et services financiers liés aux opérations bancaires — Spécifications liées à l'authentification des messages (service aux particuliers)

1 Domaine d'application

La présente Norme internationale prescrit des procédures à utiliser pour protéger l'intégrité des messages du service aux particuliers et pour vérifier que le message a pour origine une source autorisée. Elle décrit également la méthode permettant d'approuver les algorithmes utilisés pour l'authentification des messages du service aux particuliers.

Les règles relatives à la représentation des données ne sont pas spécifiées bien qu'il soit nécessaire que les deux correspondants utilisent les mêmes manières de représenter les données. Les procédures sont également indépendantes du processus de transmission utilisé.

Une liste des algorithmes approuvés pour le calcul du code d'authentification de message (MAC) est donnée dans l'annexe A. La méthode à utiliser pour approuver les algorithmes d'authentification est donnée dans l'annexe B. La procédure permettant d'empêcher toute détermination exhaustive des clés est donnée dans l'annexe C.

L'annexe D fournit un guide pour le choix des éléments d'authentification. L'annexe E donne des informations générales sur la protection contre la fraude interne de l'expéditeur et du destinataire, par exemple falsification d'un code d'authentification de message (MAC) par le destinataire, tandis que l'annexe F décrit une méthode pour la génération de clé pseudo-aléatoire. L'annexe G donne des références bibliographiques.

La présente Norme internationale ne prescrit pas

a) le chiffrement pour la protection des messages contre toute divulgation non autorisée; ni

b) la protection contre la perte ou la duplication des messages, qu'elle soit accidentelle ou intentionnelle.

La présente Norme internationale s'adresse aux institutions responsables de la mise en œuvre de techniques permettant l'authentification de messages utilisés dans le service aux particuliers.

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 8730:1990, *Opérations bancaires — Spécifications liées à l'authentification des messages.*

ISO 8731-1:1987, *Banque — Algorithmes approuvés pour l'authentification des messages — Partie 1: DEA.*

ISO 8731-2:1987, *Banque — Algorithmes approuvés pour l'authentification des messages — Partie 2: Algorithme d'authentification des messages.*

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions suivantes s'appliquent.

3.1 algorithme: Processus mathématique de calcul spécifié.

3.2 authentification: Méthode employée par un expéditeur et un destinataire pour s'assurer de l'inté-

grité des données et fournir un moyen d'authentifier leur origine.

3.3 algorithme d'authentification: Algorithme utilisé conjointement à une clé d'authentification et un ou plusieurs éléments d'authentification, à des fins d'authentification.

3.4 élément d'authentification: Élément de message qui doit à être protégé par authentification.

3.5 clé d'authentification: Clé de chiffrement utilisée pour l'authentification.

3.6 clé de chiffrement: Paramètre complémentaire d'un algorithme, servant à la validation, l'authentification, le chiffrement ou le déchiffrement.

3.7 cryptopériode: Période de validité d'une clé donnée peut être utilisée ou durant laquelle les clés d'un système donné restent valides.

3.8 chiffrement: Processus de transformation d'un texte en clair en un texte chiffré à des fins de sécurité ou de confidentialité.

3.9 code d'authentification de message (MAC): Code figurant dans un message entre l'expéditeur et le destinataire pour en valider l'origine ainsi que tout ou partie du texte du message. Le code est le résultat d'une méthode de calcul agréée.

3.10 élément de message: Groupe de bits consécutifs attribués à des fins spécifiques.

3.11 destinataire: Entité destinée à recevoir le message.

3.12 expéditeur: Entité dûment autorisée et responsable de l'envoi du message.

4 Procédures d'authentification de messages

4.1 Clés d'authentification

Les clés d'authentification sont des clés de chiffrement secrètes qui ont été préalablement échangées entre l'expéditeur et le destinataire et sont utilisées par l'algorithme d'authentification. Ces clés peuvent être générées de façon aléatoire ou pseudo-aléatoire (voir annexe F). Les clés utilisées pour les messages d'authentification ne doivent pas être utilisées à d'autres fins. Toute clé utilisée pour l'authentification doit être protégée contre toute divulgation à des tiers non autorisés.

4.2 Éléments d'authentification

Le calcul du MAC doit comprendre tous les éléments de message, spécifiés par un accord bilatéral entre l'expéditeur et le destinataire, qui doivent faire l'objet d'une protection contre une altération frauduleuse.

NOTES

1 Il est recommandé d'inclure tous les éléments de message dans le calcul du MAC.

2 Des éléments non transmis peuvent être inclus dans le calcul du MAC.

Les informations d'en-tête et de fin de message utilisées pour la transmission doivent être négligées dans le calcul du MAC.

4.3 Longueur du MAC

La longueur du MAC doit être de 32 bits.

4.4 Génération du MAC

Les algorithmes d'authentification doivent être utilisés avec la clé d'authentification et les éléments d'authentification. Le MAC doit être généré conformément aux règles de calcul d'un algorithme d'authentification approuvé, comme convenu entre l'expéditeur et le destinataire.

NOTES

3 Voir, en annexe A, la liste des algorithmes d'authentification approuvés.

4 Un changement dans la séquence des éléments d'authentification, ou dans leur représentation, après la génération du MAC, se traduira par un défaut d'authentification.

4.5 Position du MAC

Le MAC doit être soit

a) placé dans le message, dans la zone réservé au transport du MAC; ou

b) s'il n'y a pas de zone spécifique pour le MAC, placé à la suite des éléments de données du message.

Lorsque la zone allouée au MAC a une longueur, pour la transmission, supérieure à 32 bits, le MAC doit être justifié à gauche dans cette zone.

5 Vérification du MAC

Pour vérifier l'intégrité d'un message comportant un MAC le destinataire doit calculer un MAC (MAC de référence) en utilisant la méthode de calcul spéci-

fiée en 4.4 et en utilisant dans une séquence identique des données identiques aux éléments d'authentification, la même clé d'authentification et le même algorithme d'authentification. La zone contenant le MAC reçu ne doit pas être incluse dans le calcul du MAC de référence.

Le MAC de référence et le MAC reçu doivent être comparés. Leur identité permet de confirmer l'intégrité des éléments d'authentification et qu'ils ont été adressés par un expéditeur autorisé.

6 Procédure d'approbation pour algorithmes d'authentification

Avant qu'un algorithme d'authentification puisse être intégré à l'annexe A, il doit satisfaire aux deux exigences de base suivantes:

a) il doit être conçu pour satisfaire un besoin qui n'est pas déjà satisfait par les algorithmes spécifiés dans l'annexe A, par exemple convenir à un environnement opérationnel différent, ou permettre une réduction sensible des coûts de mise en œuvre ou de fonctionnement, ou, enfin offrir une protection notablement meilleure;

b) il doit être suffisamment sûr pour remplir sa mission.

L'annexe B indique comment ces objectifs doivent être réalisés.

Annexe A
(normative)

Algorithmes approuvés pour le calcul du MAC destiné à l'authentification des messages de service aux particuliers

Le(s) algorithme(s) et mode(s) d'opération(s) suivant(s) ont été approuvés pour une utilisation conjointe avec la présente Norme (voir annexe B pour de plus amples informations sur le processus d'approbation):

— l'algorithme décrit dans l'ISO 8731-1 utilisant le mode d'opération de chaînage de bloc chiffré;

NOTE 5 Voir, en annexe C, la procédure complémentaire visant à empêcher une détermination exhaustive des clés.

— l'algorithme décrit dans l'ISO 8731-2.

Annexe B
(normative)

Procédures d'examen d'autres algorithmes d'authentification

B.1 Initiative

Tout nouvel algorithme d'authentification destiné à être incorporé dans l'annexe A de la présente Norme internationale doit être soumis par un organisme national de normalisation, ou avec l'accord de celui-ci, au Secrétariat de l'ISO/TC 68.

B.2 Fondement de la proposition

Le demandeur doit justifier sa proposition en décrivant

a) le but que la proposition est censée atteindre;

b) l'intérêt que présente l'algorithme par rapport à ceux déjà énumérés dans l'annexe A de la présente Norme internationale;

c) les avantages autres que ceux déjà décrits par ailleurs;

d) l'expérience acquise dans l'utilisation du nouvel algorithme.

B.3 Documentation

L'algorithme proposé doit être accompagné d'une documentation complète lorsqu'il est soumis à l'étude. Cette documentation doit comporter

a) une description complète de l'algorithme proposé;

b) une déclaration attestant que l'algorithme satisfait aux impératifs de l'article 6 ou est compatible avec eux;

c) un organigramme logique mettant en évidence les étapes successives aboutissant au calcul du MAC;

d) une définition et une explication des nouveaux termes, facteurs ou variables introduits;

e) les spécifications liées à la clé d'authentification, à son utilisation et à sa manipulation;

f) un exemple de calcul pas à pas illustrant le calcul du MAC, en utilisant un message financier classique;

g) des informations détaillées sur tous essais préalables auxquels a été soumis l'algorithme proposé, concernant en particulier sa sécurité. Ces informations doivent comprendre une description générale des méthodes d'essai utilisées, les résultats obtenus et l'identité de l'organisme ou du groupe chargé des essais et certifiant les résultats (c'est-à-dire, des informations suffisantes doivent être fournies pour permettre à un organisme indépendant de procéder aux mêmes essais et de comparer les résultats ainsi obtenus).

B.4 Publicité

Aucun algorithme soumis à l'étude ne doit faire l'objet d'une classification de sécurité. Si une demande de brevet a été faite pour l'algorithme, l'évaluation doit avoir lieu conformément aux procédures ISO[1]. Toute documentation accompagnant l'algorithme doit être considérée comme étant du domaine public et donc accessible à toute personne physique ou morale souhaitant l'examiner et l'essayer.

B.5 Examen des propositions

Toute proposition nouvelle est examinée par l'ISO et fait l'objet d'un rapport dans les 180 jours suivant la réception (voir B.6). Le rapport doit établir si la proposition est suffisament documentée, si elle a déjà été essayée avec succès et a été certifiée et si l'algorithme proposé satisfait aux conditions et spécifications de la présente Norme internationale. L'examen peut également s'accompagner d'une soumission de la proposition à enquête publique (voir B.6).

B.6 Enquête publique

Si le rapport préconise une enquête publique, les propositions jugées recevables doivent être transmises (avec l'accord du demandeur) à des organismes et institutions sélectionnées jouissant d'une notoriété internationale dans ce domaine. Ces ins-

1) *Directives CEI/ISO — Partie 2: Méthodologie pour l'élaboration des Normes internationales*, 1989, 5.7.