Norme internationale 8730

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION•МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ•ORGANISATION INTERNATIONALE DE NORMALISATION

Opérations bancaires — Spécifications liées à la normalisation de l'authentification des messages

Banking — Requirements for message authentication (wholesale)

Première édition — 1986-11-15

CDU 336.717.131.3 **Réf. nº : ISO 8730-1986 (F)**

Descripteurs : banque, document bancaire, message, authentification.

Prix basé sur 7 pages

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 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.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour approbation, avant leur acceptation comme Normes internationales par le Conseil de l'ISO. Les Normes internationales sont approuvées conformément aux procédures de l'ISO qui requièrent l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 8730 a été élaborée par le comité technique ISO/TC 68, *Banque.*

L'attention des utilisateurs est attirée sur le fait que toutes les Normes internationales sont de temps en temps soumises à révision et que toute référence faite à une autre Norme internationale dans le présent document implique qu'il s'agit, sauf indication contraire, de la dernière édition.

Imprimé en Suisse

Opérations bancaires — Spécifications liées à la normalisation de l'authentification des messages

0 Introduction

Un code d'authentification de message (MAC) est une zone de données annexée à un ensemble de données (ou message) échangé entre des institutions financières et transmis avec cet ensemble de données. Il découle du message complet ou de certains éléments spécifiés dans le message devant être protégés contre une altération accidentelle ou frauduleuse.

Le niveau de protection offert par un algorithme donné dépend d'une part de la longueur du code d'authentification de message (MAC) et de la clé d'authentification et, d'autre part, de la possibilité qu'ont les deux correspondants de préserver la confidentialité de leur clé d'authentification. La mise en œuvre de la présente Norme internationale implique l'adhésion des correspondants à ces principes. La liste des algorithmes approuvés figure dans l'ISO 8731. Les techniques de sécurité seront décrites dans une future Norme internationale. La fiabilité mathématique d'un algorithme normal est calculée en partant du principe que le fraudeur potentiel est confronté à un grand nombre de messages en clair, contenant chacun son MAC associé, calculé d'après une clé d'authentification constante. La fiabilité est alors égale à la puissance de calcul nécessaire au fraudeur pour déterminer la clé d'authentification. Le changement fréquent de clé doit garantir une inviolabilité quasi totale du MAC, c'est-à-dire qu'il ne pourra être calculé durant la période de validité de la clé.

1 Objet

La présente Norme internationale spécifie les méthodes à utiliser pour protéger l'authenticité de messages liés à l'activité d'entreprise échangés par des institutions financières (entre banques, entre une banque et une société ou un gouvernement), en recourant à un code d'authentification de messages (MAC). Elle spécifie la méthode d'approbation des algorithmes d'authentification en vue de leur intégration à l'ISO 8731. L'application de la présente Norme internationale n'est pas une garantie contre la fraude interne, qu'elle soit du fait de l'expéditeur ou du destinataire (contrefaçon d'un MAC par le destinataire).

La présente Norme internationale spécifie une technique de protection de message, dans sa totalité ou dans certains de ses éléments. Ces spécifications peuvent être complétées par un groupe d'institutions financières présentant des intérêts communs et qui ont pris des dispositions fonctionnelles propres (par exemple un consortium bancaire, un regroupement géographique, un réseau d'exploitation, un accord de secteur industriel). L'authentification des messages est indépendante du système de transmission utilisé.

La présente Norme internationale vise l'utilisation d'algorithmes symétriques, expéditeur et destinataire utilisant la même clé. Elle s'applique à des messages formatés et transmis sous forme de jeux de caractères codés. Des dispositions seront prises en temps utile pour traiter de l'emploi d'algorithmes asymétriques et de la transmission de messages en binaire.

La présente Norme internationale n'indique pas de méthode de protection contre la duplication, la perte d'information ou la lecture et la surveillance non autorisées. L'annexe B contient une méthode de protection contre la duplication et la perte.

NOTE — Le chiffrage des messages constitue une méthode de protection contre la lecture et la surveillance non autorisées.

2 Domaine d'application

La présente Norme internationale s'adresse à des institutions financières échangeant des messages. Elle peut également convenir à d'autres institutions non-financières devant également émettre ou recevoir des messages. Elle peut servir à authentifier des messages transmis par un service de télécommunication ou un autre moyen de transmission.

3 Références

ISO 646, *Traitement de l'information — Jeu ISO de caractères codés à 7 éléments pour l'échange d'information.*

ISO 2014, *Représentation numérique des dates.*

ISO 7982, *Télécommunication bancaire — Messages de transferts de fonds — Vocabulaire et éléments de données.* [1)]

ISO 8227, *Traitement de l'information — Chiffrement des données — Spécification de l'algorithme DEA 1.* [1)]

ISO 8731, *Banque — Algorithmes approuvés pour l'authentification des messages.* [1)]

1) Actuellement au stade de projet.

4 Définitions

Dans le cadre de la présente Norme internationale, les définitions suivantes sont applicables.

4.1 algorithmes : Processus mathématique clairement énoncé propre à un calcul; un ensemble de règles dont l'application donne un résultat déterminé.

4.2 authentification : Technique appliquée par l'expéditeur et le destinataire pour valider l'origine et le texte complet ou partiel d'un message.

4.3 algorithme d'authentification : Processus mathématique dont le résultat dépend du texte (énoncé en clair ou chiffré) et de la clé d'authentification qu'il inclut.

4.4 élément d'authentification : Suite ininterrompue de caractères devant être protégée, en lui appliquant l'*algorithme d'authentification*.

4.5 clé d'authentification : Clé cryptographique dont seuls les correspondants ont connaissance. Si l'on applique cette clé et le texte du message à l'*algorithme d'authentification,* on obtient le *code d'authentification de message (MAC).*

4.6 partie(s) bénéficiaire(s) : La ou les parties qui doivent être créditées ou payées à l'aboutissement d'un transfert.

4.7 polarisation : Phénomène lié à la création de nombres aléatoires ou pseudo-aléatoires dans un intervalle donné, faisant que certains nombres sortent plus souvent que d'autres.

4.8 date de calcul du MAC : Date à laquelle l'*expéditeur* calcule le *MAC.*

4.9 délimiteurs : Groupe de caractères servant à marquer le début et la fin des données.

4.10 double contrôle : Intervention d'au moins deux entités (généralement des personnes), opérant de concert, pour protéger des fonctions ou des informations sensibles, aucune personne ne pouvant seule accéder à des (ou utiliser les) données; par exemple clé cryptographique.

4.11 chiffre hexadécimal : Caractère unique choisi dans l'intervalle 0-9, A-F (majuscule) représentant une composition de quatre éléments binaires.

4.12 code d'authentification de message (MAC) : Zone de données dont le contenu peut servir à vérifier l'authenticité d'un message.

4.13 identificateur de message (MID) : Zone comprenant au maximum seize caractères alphanumériques servant à identifier sans ambiguïté un message financier ou une transaction.

4.14 texte du message : Informations acheminées ou transmises entre l'expéditeur et le destinataire, en excluant les informations d'en-tête et de fin, liées à la transmission.

4.15 destinataire : Personne, institution ou autre entité responsable de la réception du message.

4.16 expéditeur : Personne, institution ou autre entité dûment autorisée et responsable de l'envoi du message.

4.17 date de valeur : Date à laquelle les fonds doivent être à la disposition du destinataire.

4.18 service de télécommunication : Tout service de télécommunication autorisant l'échange de message entre abonnés (exemple Télex, TWX, S.W.I.F.T., Fedwire ainsi que tout autre réseau public ou privé).

5 Protection

5.1 Protection de l'identité de l'expéditeur et du destinataire

Afin de protéger l'identité de l'expéditeur et du destinataire, la clé d'authentification doit être protégée et son utilisation doit être restreinte à ces deux parties uniquement (ou leurs représentants attitrés).

5.2 Éléments d'authentification

5.2.1 Les éléments d'authentification suivants doivent toujours être inclus dans le calcul du MAC

a) date de calcul du MAC;

b) identificateur de message (MID).

5.2.2 Les éléments d'authentification suivants doivent toujours être inclus dans le calcul du MAC, lorsqu'ils apparaissent dans le message

a) montant de la transaction;

b) monnaie;

c) identification des parties à créditer et à débiter;

d) identification du bénéficiaire;

e) date de valeur.

5.3 Protection du message dans son ensemble

Lorsque les correspondants souhaitent protéger le texte complet du message, le processus d'authentification doit s'appliquer au texte entier (voir 7.1.1).

6 Création et traitement du code d'authentification de message (MAC)

L'expéditeur d'un message doit générer un MAC en intégrant (dans l'ordre où ils apparaissent dans le message) les éléments d'authentification des messages transmis qui doivent être protégés dans un algorithme d'authentification normalisé. Puis

l'algorithme est mis en action, grâce à une clé d'authentification échangée préalablement avec le destinataire et qui n'est connue que des deux correspondants. Ce processus donne naissance au MAC, qui est inclus dans le message original en clair, en tant que zone de données supplémentaires. A la réception du message, le destinataire calcule un MAC de référence, en utilisant des données identiques aux éléments de données protégés, une clé d'authentification identique et un algorithme identique. L'authenticité des éléments de données du message reçu est confirmée, lorsque le MAC de référence calculé par le destinataire correspond à celui qui accompagne le message.

Un MAC reçu (ainsi que ses délimiteurs) ne doivent pas être inclus dans le calcul de l'algorithme.

7 Procédures d'authentification de message

7.1 Processus d'authentification

Les correspondants doivent convenir de l'algorithme à appliquer et aussi échanger une clé confidentielle d'authentification. L'expéditeur calcule alors un MAC utilisant ces éléments. Le MAC doit être inclus dans le corps du message transmis, de telle sorte qu'il puisse être identifié par le destinataire.

7.1.1 Texte complet du message

Sauf dans le cas spécifié en 7.1.2, l'algorithme d'authentification doit être appliqué à la totalité du texte du message.

7.1.2 Éléments choisis du message

Lorsque l'authentification du message complet n'est pas réalisable, l'algorithme ne doit être appliqué qu'aux éléments d'authentification spécifiés (voir 5.2). Ces éléments doivent être mis en évidence en recourant aux techniques décrites en 7.4.

7.1.2.1 Les éléments d'authentification doivent être considérés dans l'ordre où ils apparaissent dans le message.

7.1.2.2 L'émetteur doit choisir la clé d'authentification pour le destinaire en fonction de la date, qui doit également figurer dans le message (voir 7.3).

7.1.2.3 Les critères de mise en forme décrits en 7.4.3 doivent être appliqués.

7.1.2.4 Les éléments d'authentification une fois mis en forme sont soumis à l'algorithme.

7.1.2.5 Le MAC obtenu doit être ajouté au message avant la transmission.

7.1.2.6 Le destinataire doit répéter les opérations d'extraction et de calcul. Les éléments des messages doivent être considérés comme authentifiés si le MAC de référence obtenu est identique à celui que contenait le message reçu.

7.2 Création d'une clé d'authentification

Les clés d'authentification doivent être obtenues par une opération aléatoire ou pseudo-aléatoire de sorte que

a) les séquences d'éléments (par exemple les éléments binaires) constituant la clé aient toutes une chance égale d'être générées, de sorte que toute séquence soit l'une des probabilités de l'ensemble complet des séquences possibles;

b) aucune séquence d'éléments issue de l'algorithme de génération ne présente de corrélation avec la séquence précédente ou suivante;

c) le processus de génération soit exempt de polarisation.

NOTE — L'annexe C est un exemple de méthode permettant de répondre à ces impératifs.

Un double contrôle, s'il est mis en œuvre, doit s'effectuer par la création indépendante de deux clés préliminaires non abrégées, combinées par la fonction modulo 2, au niveau de l'appareil d'authentification placé sur chaque site.

NOTE — Cette technique suppose que personne ne peut voir quelle clé d'authentification entre dans le calcul du MAC.

7.3 Formats de zone

Les formats de zone «MAC», «date de calcul du MAC» et «identification du message» doivent avoir une représentation normalisée dans tous les messages, telle que spécifiée ci-dessous.

7.3.1 MAC

Le MAC doit être exprimé sous la forme de huit chiffres hexadécimaux de quatre bits (0-9, A-F), répartis en deux groupes séparés par un espace (hhhh hhhh); par exemple, 5A6F O9C3.

7.3.2 Date de création du message

La date à laquelle l'institution expéditrice crée le message doit être exprimée conformément à l'ISO 2014, en indiquant l'année, le mois, le jour (abrégé de préférence, c'est-à-dire AAMMJJ); par exemple, 810921 pour le 21 septembre 1981.

7.3.3 Identificateur de message (MID)

L'identificateur de message doit être exprimé par un à seize caractères alphanumériques (aaaaaaaaaaaaaaaa). Les caractères autorisés sont 0-9, A-Z (majuscules), l'espace, la virgule (,), le point (.), la barre oblique (/) et le trait d'union (-); par exemple, FNBC25.

7.4 Délimitation et extraction des éléments choisis

Le processus d'authentification doit s'appliquer aux éléments d'authentification dans l'ordre où ils se présentent dans le message. Des conditions particulières régissent la délimitation

de ces éléments et la mise en forme des caractères. Un message peut contenir des éléments d'authentification délimités implicitement ou explicitement.

7.4.1 Délimiteurs implicites de zone

Un élément d'authentification est implicitement délimité si sa place dans le message est fixe ou identifiée sans ambiguïté par des règles normalisées de format. Les noms de zone, les nombres, ou les étiquettes mnémoniques d'identification doivent être pris en compte pour l'authentification, dès lors que le service de télécommunication les signale comme délimiteurs implicites.

7.4.2 Délimiteurs explicites de zone

Si on en utilise, les délimiteurs explicites doivent servir à marquer le début et la fin des éléments d'authentification. Ils doivent être utilisés tant au sein de messages de format variable que dans des zones libres de messages au format fixe.

Les délimiteurs explicites de début et de fin, s'ils existent, doivent se présenter par couples complémentaires, sans délimiteurs explicites intermédiaires. Si cette condition n'est pas remplie, le message n'est pas authentifié. Le message peut contenir un nombre quelconque de zones délimitées; toutefois, la Date et les zones MID et MAC ne doivent apparaître qu'une fois dans le message. Le trait d'union (-) doit figurer dans tous les délimiteurs explicites.

7.4.2.1 La date de création de message : QD- et -DQ

Exemple QD-AAMMJJ-DQ

7.4.2.2 L'identificateur de message (MID) : QX- et -XQ

Exemple QX-aaaaaaaaaaaaaaa-XQ

7.4.2.3 Autres éléments d'authentification : QT- et -TQ

Exemple QT-Texte-TQ. Le texte ainsi délimité peut avoir une longueur quelconque, dans la limite des possibilités du service de télécommunication. Il est soumis aux critères de mise en forme indiqués en 7.4.3.

7.4.2.4 MAC : QM- et -MQ

Exemple QM-hhhh hhhh-MQ

7.4.3 Mise en forme de texte pour le calcul du MAC

Tous les caractères des éléments d'authentification entrant dans l'algorithme doivent comporter huit éléments binaires, à savoir les 7 éléments binaires du code de l'ISO 646 précédés d'un zéro (exemple 0, b7, b6 ...bl). Si une conversion de code s'impose, celle-ci ne doit intervenir qu'à des fins de calcul interne.

Les règles de mise en forme suivantes s'appliquent dans l'ordre indiqué à tous les éléments d'authentification — implicitement et explicitement délimités — avant qu'intervienne le traitement par l'algorithme d'authentification :

7.4.3.1 Tout délimiteur explicite de début doit être supprimé et tout délimiteur explicite de fin doit être remplacé par un espace unique.

7.4.3.2 Sous réserve des dispositions du 7.4.3.6, un seul espace doit être inséré à la suite de toute zone délimitée implicitement et à la fin de chaque ligne.

7.4.3.3 Les caractères alphabétiques minuscules (a-z) sont remplacés par des majuscules (A-Z).

7.4.3.4 Tout caractère autre que les lettres A à Z, les chiffres 0 à 9, l'espace, la virgule (,), le point (.), la barre oblique (/), l'astérique (*) et le trait d'union (-) doit être supprimé. Cette règle s'applique par conséquent aux caractères de retour-chariot, d'interligne, de fin de texte et autres caractères de mise en forme et de commande.

7.4.3.5 Tous les espaces de début doivent être supprimés.

7.4.3.6 Toute suite d'espaces consécutifs (dans le corps ou la fin du texte) doit être remplacée par un seul espace.

7.5 MAC «non-reconnu»

Quand le MAC est généré automatiquement, c'est-à-dire par extraction automatique des éléments d'authentification, le non-respect des règles précitées peut faire échouer l'opération (imbrication des délimiteurs, par exemple). Dans ce cas et lorsque l'erreur doit pouvoir être constatée de façon lisible (sur papier, écran ou microfiche), l'échec de l'opération doit être signalé par huit blancs (si possible) répartis en deux groupes de quatre, séparés par un caractère autre qu'un chiffre hexadécimal tel que défini en 7.3.1; par exemple, bbbb*bbbb. Si des blancs ne sont pas disponibles, ils doivent être remplacés par des zéros; par exemple, 0000*0000.

Lorsqu'un MAC ne correspond pas au MAC de référence créé au cours du processus d'authentification, l'échec doit être indiqué par l'insertion d'un caractère d'impression non-hexadécimal à la place du blanc dans le MAC reçu. S'il est disponible dans le jeu de caractères, utiliser un astérisque; par exemple, 5A6F*09C3.

8 Procédure d'approbation de méthodes d'authentification

Avant qu'une méthode d'authentification puisse être intégrée à l'ISO 8731, elle doit répondre aux deux exigences suivantes :

a) être conçue pour une mission que ne remplit pas déjà l'ISO 8731 (par exemple convenir à un environnement différent ou permettre une réduction sensible des coûts de mise en œuvre ou de fonctionnement ou, enfin, offrir une protection notablement meilleure);

b) être suffisamment sûre, fiable et stable pour remplir sa mission.

L'annexe A indique comment atteindre ces objectifs.

Annexe A

Procédure de soumission d'autres méthodes d'authentification

(Cette annexe fait partie intégrante de la norme.)

A.1 Initiative

Toute méthode alternative d'authentification visant à être incorporée dans l'ISO 8731 doit être soumise par un organisme national de normalisation ou avec l'accord de celui-ci au Secrétariat de l'ISO/TC 68.

A.2 Fondement de la proposition

Le demandeur doit justifier sa proposition en décrivant :

a) la mission que doit remplir la méthode;

b) l'intérêt que présente la méthode par rapport à celles que décrit déjà l'ISO 8731;

c) les avantages autres que ceux déjà décrits;

d) l'expérience acquise dans l'utilisation de la nouvelle méthode.

A.3 Documentation

Un document complet doit accompagner la méthode soumise à considération. Cette documentation doit comprendre :

a) une description complète de la méthode proposée;

b) une déclaration attestant clairement que la méthode répond aux impératifs du chapitre 5 ou est compatible avec lui;

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

d) une définition, avec commentaire à l'appui, de tout nouveau terme, facteur ou variable;

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

f) un exemple de calcul pas à pas, illustrant le calcul du MAC, à l'appui d'un message financier classique;

g) des informations détaillées sur tout essai préalable auquel la méthode aurait été soumise, concernant notamment sa sécurité, sa fiabilité et sa stabilité. Ces informations devraient comprendre une description générale des procédures d'essai utilisées, les résultats obtenus et l'identité de l'organisme ou du groupe effectuant les essais et certifiant les résultats (en résumé, des informations suffisantes devraient permettre à un organisme indépendant de procéder aux mêmes essais et de comparer les résultats obtenus).

A.4 Publicité

Aucune méthode soumise à l'étude ne doit faire l'objet d'une classification de sécurité. Si la méthode a été brevetée, l'évaluation doit avoir lieu conformément aux procédures ISO[1]. Toute documentation et information accompagnant la demande d'étude de la méthode sera considérée comme étant du domaine public et donc accessible à toute personne physique ou morale souhaitant en prendre connaissance, l'essayer et l'utiliser.

A.5 Examen des propositions

Toute proposition nouvelle sera examinée par l'ISO et fera l'objet d'un compte rendu dans les 180 jours suivant la réception (voir également A.6). Ce rapport doit établir si la proposition est suffisamment documentée, si elle a déjà été essayée correctement et certifiée et si la méthode proposée répond aux conditions et spécifications énoncées dans la présente Norme internationale. Le rapport peut également demander que la proposition soit rendue publique (voir A.6).

A.6 Examen public

Si le compte rendu (A.5) recommande un examen public, les propositions jugées recevables doivent être transmises (avec l'accord du demandeur) à des organismes et institutions sélectionnés jouissant d'une notoriété internationale dans ce domaine. Ces instances doivent rendre leur avis dans les 90 jours suivant la réception de la proposition.

NOTE — Cette période d'examen public peut s'ajouter aux 180 jours prévus pour la préparation du compte rendu de la proposition (voir A.5).

A.7 Procédure d'appel

Les demandeurs dont les propositions sont rejetées (voir A.5), peuvent demander au Secrétariat de l'ISO/TC68 que leur proposition soit soumise à la procédure d'examen public (voir A.6), si cela n'a pas encore été fait. Si, au terme de cet examen public, le rejet est toujours recommandé, le demandeur peut solliciter auprès du secrétariat de l'ISO/TC68 une distribution de sa proposition, accompagnée des rapports la concernant, pour vote, afin que les membres P du sous-comité

1) Directives pour les travaux techniques de l'ISO, 14ème édition (1985), annexe 1E.