NORME INTERNATIONALE

ISO 8730

Deuxième édition
1990-05-15

Opérations bancaires — Spécifications liées à l'authentification des messages

Banking — Requirements for message authentication (wholesale)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9cc-d39e3cf6805b/iso-8730-1990

Numéro de référence
ISO 8730:1990(F)

Sommaire

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9cc-d39e3cf6805b/iso-8730-1990

© ISO 1990
Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

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 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b847692a-4ef6-4d09-b9cc-d39e3cf6805b/iso-8730-1990

La Norme internationale ISO 8730 a été élaborée par le comité technique ISO/TC 68, *Banque et services financiers liés aux opérations bancaires*.

Cette deuxième édition annule et remplace la première édition (ISO 8730-1:1986), qui a fait l'objet d'une révision technique afin de clarifier les améliorations déjà apportées dans cette édition.

Ces améliorations sont déjà apportées dans le document ANSI X9.9 publié en août 1986 et le nouveau texte reste cohérent avec le texte publié par l'ANSI.

Les changements spécifiques apportés dans la présente édition sont:

a) les données présentées pour authentification peuvent être formatées de cinq manières différentes. Le processus de choix permet aux utilisateurs d'authentifier les messages selon l'option de format qui convient le mieux au processus de transmission utilisé;

   Les correspondants doivent maintenant se mettre d'accord sur l'option de format pour l'authentification de tout message particulier, ceci ne devenant pas en fait une obligation majeure pour les parties concernées étant donné que le mode de sélection sera déterminé par le choix du processus de transmission;

b) introduction d'une nouvelle zone permettant d'identifier la clé d'authentification utilisée (zone IDA);

c) plusieurs définitions ont aussi été modifiées afin d'assurer la cohérence avec les autres Normes internationales du TC 68.

Dans le même temps quatre nouvelles annexes ont été ajoutées, toutes dans l'intention de simplifier la mise en œuvre de la présente Norme internationale:

a) l'annexe B décrit les risques associés à l'introduction accidentelle de caractères de contrôle au cours du processus de reformatage et la manière dont ces risques peuvent être réduits;

b) l'annexe D et l'annexe E fournissent des exemples de calcul d'authentification au moyen des algorithmes spécifiés dans l'ISO 8731:1987, Parties 1 et 2;

c) l'annexe F décrit un moyen d'application de la présente Norme internationale à un ordre de paiement par télex formaté conformément aux presciptions de l'ISO 7746.

L'annexe A fait partie intégrante de la présente Norme internationale. Les annexes B et C et D et E et F et G sont données uniquement à titre d'information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9cc-d39e3cf6805b/iso-8730-1990

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.

Quelle que soit la nature de l'altération, 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 gestion de clé sont spécifiées dans l'ISO 8732. La fiabilité mathématique d'un algorithme normalisé est calculée en partant du principe que le fraudeur potentiel est confronté à un nombre arbitrairement grand de messages en clair, contenant chacun son MAC associé, calculé d'après une même clé d'authentification. La fiabilité est alors déterminée par la puissance de calcul nécessaire au fraudeur pour déterminer la clé d'authentification et par la longueur du MAC.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b847f69a5-4eb6-4d09-b9cc-d39e3cf6805b/iso-8730-1990

Page blanche

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9cc-d39e3cf6805b/iso-8730-1990

Opérations bancaires — Spécifications liées à l'authentification des messages

1 Domaine d'application

La présente Norme internationale est conçue pour être utilisée par des institutions échangeant des messages financiers. Elle peut servir à authentifier des messages transmis par un service de télécommunication ou tout autre mode de transmission.

La présente Norme internationale spécifie les méthodes à utiliser pour protéger l'authenticité de messages financiers liés à l'activité d'entreprise échangés par des institutions (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, par exemple la 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. Les données présentées à l'authentification peuvent être formatées sous une forme à choisir parmi cinq options. 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). Le choix de l'option appropriée permet une authentification des messages compatibles avec le système de transmission utilisé.

La protection de l'intégrité s'applique uniquement aux éléments d'authentification choisis. Les altérations des autres parties du message ne sont pas décelées. Il incombe aux utilisateurs de garantir l'intégrité de la présentation des données (voir annexe B). La présente Norme internationale offre un moyen de protection contre la répétition et la perte; une méthode est décrite à l'annexe C.

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

La présente Norme internationale n'indique pas de méthode de protection contre la lecture et la manipulation non autorisées, telle quelle peut être obtenue par chiffrement du message comme décrit dans l'ISO 10126[1].

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/...
d39e3cf68f5b/iso-8730-1990

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 646:1983, *Traitement de l'information — Jeu ISO de caractères codés à 7 éléments pour l'échange d'information.*

ISO 7746:1988, *Banque — Messages télex interbancaires.*

1) À publier.

ISO 7982-1:1987, *Télécommunication bancaire — Messages de transfert de fonds — Partie 1: Vocabulaire et éléments de données.*

ISO 8601:1988, *Éléments de données et formats d'échange — Échange d'information — Représentation de la date et de l'heure.*

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

ISO 8732:1988, *Banque — Gestion de clés.*

ISO 10126-1:—[2], *Banque — Procédures de chiffrement de message — Partie 1: Principes généraux.*

ISO 10126-2:—[2], *Banque — Procédures de chiffrement de message — Partie 2: Algorithmes.*

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions suivantes s'appliquent. Les termes imprimés en italique dans les définitions sont définis ailleurs dans le présent article.

3.1 algorithme: Processus mathématique propre à un calcul; un ensemble de règles dont l'application donne un résultat déterminé.

3.2 authentification: Processus appliqué par l'expéditeur et le destinataire pour garantir l'*intégrité des données* et fournir l'*authentification de l'origine des données*.

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* que l'on désire protéger par l'*authentification*.

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

3.6 bénéficiaire(s): Le ou les interlocuteur(s) qui doit/doivent être crédité(s) ou payé(s) à l'aboutissement d'un transfert.

3.7 biais: La situation dans laquelle au cours de la création de nombres aléatoires ou pseudo-aléatoires, certains nombres sortent plus souvent que d'autres.

3.8 période de validité: Période de temps définie au cours de laquelle une clé de chiffrement spécifique peut être utilisée, ou au cours de laquelle les clés de chiffrement peuvent rester efficaces dans un système donné.

3.9 intégrité des données: Capacité qu'ont des données de ne pas pouvoir être altérées ou détruites d'une manière frauduleuse.

3.10 date de calcul du MAC (DMC): Date à laquelle l'*expéditeur* calcule le *code d'authentification de message*. Cette date peut être utilisée pour synchroniser le processus d'authentification en choisissant la clé appropriée.

3.11 authentification de l'origine des données: Confirmation que la source des données reçues est celle revendiquée.

3.12 déchiffrement: L'inverse du *chiffrement* reversible correspondant.

3.13 décryptage: voir *déchiffrement*.

3.14 délimiteur: Groupe de caractères servant à marquer le début et la fin d'une ou plusieurs zones de données.

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

3.16 chiffrement: Transformation cryptographique de données en vue de produire un texte chiffré.

3.17 cryptage: voir *chiffrement*.

3.18 chiffre hexadécimal: Caractère unique choisi dans l'intervalle 0-9, A-F (majuscule), représentant une série de quatre éléments binaires, comme suit:

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9cc-d20e3cf6805b/iso-8730-1990

2) À publier.

Binaire	Décimal	Héxadécimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

3.19 identificateur de clé d'authentification (IDA): Zone qui identifie la clé à utiliser pour authentifier le message.

3.20 code d'authentification de message (MAC): Code contenu dans un message entre un expéditeur et un destinataire, utilisé pour valider la source et une partie ou l'ensemble du texte du message. Le code est le résultat d'un calcul ayant fait l'objet d'un accord.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9cc-d39e3cf6805b/iso-8730-1990

3.21 élément de message: Groupe de caractères contigus utilisable dans un but spécifique.

3.22 identificateur de message (MID): Zone utilisée pour identifier de manière unique un message financier ou une transaction (exemple, référence de la transaction de la banque expéditrice).

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

3.24 destinataire: Personne, institution ou autre entité dûment autorisée et responsable de la réception du message.

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

3.26 date de valeur: Date à laquelle les fonds doivent être à la disposition du bénéficiaire.

3.27 service de télécommunication: Tout service de télécommunication autorisant l'échange de messages entre abonnés.

4 Protection

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

Afin d'empêcher l'usurpation d'identité de l'expéditeur, la clé d'authentification doit être protégée et son utilisation doit être restreinte à l'expéditeur et au destinataire (ou leurs représentants attitrés).

4.2 Éléments d'authentification

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

a) date de calcul du MAC (DMC);

b) identificateur de message (MID).

4.2.2 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) devise;

c) identificateur de clé d'authentification (IDA);

d) identification des entités à créditer et à débiter;

e) identification du bénéficiaire;

f) date de valeur.

4.3 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 6.5 et 6.7).

4.4 Protection contre la répétition et la perte

Pour assurer la protection contre la répétition et la perte, une référence unique de transaction (ou identificateur de message) doit être utilisée. L'identificateur de message (MID) est une valeur qui n'est pas répétée avant (i) le changement de date (c'est-à-dire la date de calcul du MAC), ou (ii) l'expiration de la période de validité de la clé utilisée pour l'authentification, selon l'événement survenant le premier, c'est-à-dire qu'il ne doit pas y avoir plus d'un message avec la même date et le même identificateur de message utilisant la même clé. Cette exigence peut être satisfaite par l'inclusion d'un numéro de référence unique pour la transaction de la banque expéditrice dans un message à format fixe servant d'identificateur de message.

Dans les messages de format libre, la zone du MID doit être délimitée conformément à la présente Norme internationale (voir 6.3.1). Une méthode de protection est donnée à l'annexe C.

5 Génération et vérification du code d'authentification de message (MAC)

5.1 Génération

L'expéditeur d'un message doit générer un MAC en traitant (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 approuvé (voir ISO 8731). L'algorithme doit fonctionner avec 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 doit être inclus dans le texte du message original, en tant que zone de données supplémentaires.

5.2 Vérification

À la réception du message, le destinataire doit calculer un MAC de référence, en utilisant les éléments d'authentification, une clé d'authentification identique et un algorithme identique. L'authenticité des éléments d'authentification et la source du message sont confirmés lorsque le MAC de référence calculé par le destinataire correspond à celui qui accompagne le message.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84760a5-4e0f-4d0b-b9ea-d39e3cf6805b/iso-8730-1990

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

Lorsque le MAC reçu ne correspond pas au MAC de référence calculé, le défaut d'authentification doit être communiqué conformément à 6.9.2.

Le processus de génération du MAC est sensible à l'ordre dans lequel les éléments d'authentification sont transmis, c'est-à-dire qu'un changement intervenant dans l'ordre des éléments d'authentification après la génération du MAC se traduit par un défaut d'authentification.

Les clés d'authentification du message ne doivent pas être utilisées comme clés de chiffrement.

6 Procédures d'authentification de message

6.1 Processus d'authentification

Les correspondants doivent convenir de l'algorithme à appliquer et aussi échanger une clé d'authentification secrète. L'expéditeur calcule alors un MAC utilisant ces éléments. Le MAC doir être joint au texte du message transmis, de telle sorte qu'il puisse être identifié par le destinataire. (Pour les messages de format libre voir 6.3.3.) Le destinataire répète le calcul en utilisant la même méthode d'authentification que celle décrite dans cette section. Le message est authentifié si le MAC reçu et le MAC de référence calculé sont identiques.

6.2 Options de format

La présente Norme internationale offre cinq options pour le format des données à authentifier:

1) données binaires; (6.4);

2) caractères codés; (6.5); texte complet du message, pas de mise en page

3) caractères codés; (6.6); éléments extraits du message, pas de mise en page

4) caractères codés; (6.7); texte complet du message; mise en page

5) caractères codés; (6.8); éléments extraits du message; mise en page

L'option 1 est conçue pour authentifier une chaîne binaire de données.

Les options 2 et 3 sont conçues pour authentifier les données sous forme de jeux de caractères codés chaque fois que le moyen de transmission offre une transparence au jeu de caractères, par exemple systèmes et réseaux conçus conformément au modèle des systèmes ouverts interconnectés (OSI).

Les options 4 et 5 sont conçues pour l'authentification des données sous forme d'un jeu restreint de caractères codés utilisé lorsque le moyen de transmission n'est pas transparent au jeu de caractères utilisé, par exemple code baudot, telex et services de commutation tels que ceux offerts par de nombreux services internationaux de communication.

Le choix de l'option de format incombe aux correspondants et doit faire l'objet d'un accord bilatéral.

6.3 Jeux de caractères codés (comme ceux utilisés dans les options 2 à 5)

6.3.1 Formats définis des éléments de message

Les formats de zone pour la date de calcul du MAC, l'identificateur de clé d'authentification, le code d'authentification de message et l'identificateur de message sont représentés sous la forme spécifiée dans la présente Norme internationale. Les formats pour les autres éléments de message ne sont pas spécifiés.

Les formats de zone doivent être vérifiés comme partie intégrante du processus d'authentification. Si

l'option d'authentification avec mise en page est choisie, les formats de zone doivent être vérifiés avant la mise en page. S'il se produit une erreur de formatage, le message ne sera pas authentifié. Les formats de zone suivants apparaissent comme indiqué:

a) Date de calcul du MAC (DMC). La date à laquelle l'institution expéditrice crée le message doit être exprimée conformément à l'ISO 8601 sous la forme année, mois, jour (de préférence sous forme abrégée, à savoir AAMMJJ), par exemple 851101 pour 1 novembre 1985.

b) Identificateur de clé d'authentification (IDA). Cette zone est l'identificateur de la clé d'authentification qui doit être conforme aux exigences relatives aux identificateurs de clés spécifiées dans l'ISO 8732. Permet de laisser un message dans le texte sans qu'il apparaisse à l'impression.

c) Code d'authentification de message (MAC). Le MAC doit être exprimé sous forme de huit chiffres hexadécimaux répartis en deux groupes de quatre, séparés par un blanc (hhhhbhhhh), par exemple 5A6Fb09C3.

d) Identificateur de message (MID). L'identificateur de message doit être exprimé sous forme de un à seize caractères imprimables (aaaaaaaaaaaaaaaa). Les caractères autorisés sont 0-9, A-Z (majuscules), l'espace (b), la virgule (,), le point (.), la barre oblique (/), l'astérisque (*) et le trait d'union (-); par exemple FN-BC/2.5.

6.3.2 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.

6.3.3 Délimiteurs explicites de zone

Les délimiteurs explicites peuvent être utilisés pour identifier le début et la fin des éléments de message, y compris le MAC. Ils peuvent être utilisés dans toutes les options de jeux de caractères codés. Les délimiteurs explicites suivants sont spécifiés:

a) Date de calcul du MAC (DMC): QD- et -DQ, exemple: QD-AAMMJJ-DQ;

b) Identificateur de clé d'authentification (IDA): QK- et -KQ, exemple: QK-1357BANKATOBANKB-KQ;

c) Code d'authentification de message (MAC): QM- et -MQ exemple: QM-hhhhbhhhh-MQ;

d) Identificateur de message (MID): QX- et -XQ exemple: QX-aaaaaaaaaaaaaaaa-XQ; et

e) Autres éléments de message: QT- et -TQ exemple: QT-texte-TQ

Le «texte» délimité dans QT-texte-TQ peut avoir n'importe quelle longueur autorisée par le service de télécommunication.

6.3.4 Utilisation des délimiteurs

Les délimiteurs explicites de début et de fin, s'ils existent, doivent se présenter par couples complémentaires, sans délimiteurs explicites intermédiaires.

NOTE 1 Si cette condition n'est pas remplie, le message n'est pas authentifié.

Le message peut contenir un nombre quelconque de zones de «texte» délimitées, toutefois, les zones des DMC, MID, IDA et du MAC ne doivent apparaître qu'une fois dans le message.

Le trait d'union (-) doit figurer dans tous les délimiteurs explicites.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/...-d3923cf6805b/iso-8730-1990

6.3.5 Représentation des caractères

Tous les caractères des éléments d'authentification qui sont introduits dans l'algorithme doivent être représentés par des caractères de 8 bits comprenant le jeu de caractères codés à 7 éléments de l'ISO 646 (à l'exclusion des caractères nationaux) précédé d'un zéro (par exemple 0, b7, b6, ...b1). Lorsque cela nécessite une traduction de code, la traduction ne doit servir qu'à des fins internes. Si le message est transformé en un jeu de caractères différents, la transformation inverse doit être appliquée avant que ne débute le processus d'authentification.

6.3.6 Information d'en-tête et de fin

L'information d'en-tête et de fin de message ajoutée (par exemple par un réseau) à des fins de transmission doit être omise, c'est-à-dire qu'elle ne doit pas faire partie du texte du message et ne doit pas être incluse dans le calcul de l'algorithme.

6.4 Option 1: Données binaires

L'algorithme d'authentification doit être appliqué au texte complet du message, ou à des parties du texte du message, selon l'accord bilatéral conclu entre l'expéditeur et le destinataire.

6.5 Option 2: Caractères codés; message entier; pas de mise
message entier; pas de mise en page

Lorsque le traitement du message est automatisé et que le contenu précis du corps du message ne change pas entre l'expéditeur et le destinataire, l'algorithme peut être appliqué au message entier.

Le MAC est calculé sur le texte entier du message (voir exemple en annexe D).

6.6 Option 3: Caractères codés; éléments extraits du message; pas de
éléments extraits du message; pas de mise en page

6.6.1 Utilisation

Lorsque l'authentification du message entier n'est pas possible, l'algorithme d'authentification doit être appliqué uniquement aux éléments de message choisis.

Les éléments de message doivent être extraits conformément aux règles décrites en 6.6.2. Un MAC doit être calculé sur les éléments extraits, pris dans l'ordre dans lequel ils apparaissent (voir exemple dans l'annexe D).

6.6.2 Extraction des éléments de message

Les éléments de message à authentifier doivent être extraits selon les règles suivantes:

6.6.2.1 Supprimer tous les caractères autres que les éléments du message et leurs délimiteurs correspondants.

6.6.2.2 Insérer un seul espace après chaque élément de message implicitement délimité.

6.7 Option 4: Caractères codés; message entier; mise en page
message entier; mise en page

6.7.1 Utilisation

Le MAC doit être calculé sur le texte du message à la suite de la mise en page selon les règles décrites en 6.7.2 (voir exemple dans l'annexe D).

6.7.2 Mise en page

Les règles de mise en page suivantes doivent s'appliquer dans l'ordre présenté, à tous les éléments de message — délimités implicitement ou explicitement — avant le traitement par l'algorithme d'authentification:

6.7.2.1 Chaque retour chariot et chaque changement de ligne doivent être remplacés par un seul espace.

6.7.2.2 Les caractères alphabétiques minuscules (a-z) doivent être transcrits en majuscules (A-Z).

6.7.2.3 Tous les caractères autres que les lettres A-Z, les chiffres 0-9, l'espace, la virgule (,), le point (.), la barre oblique (/), l'astérisque (*), les parenthèses de début et de fin et le trait d'union (-) doivent être supprimés. De même la fin de texte et tout autre caractères de formatage et de contrôle doivent être supprimés.

6.7.2.4 Tous les espaces d'en-tête doivent être supprimés.

6.7.2.5 Chaque série d'espaces consécutifs (internes et de fin) doit être remplacée par un seul espace.

6.8 Option 5: Caractères codés; éléments extraits du message; mise en
éléments extraits du message; mise en page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

6.8.1 Utilisation

Voir 6.6.1.

ISO 8730:1990
https://standards.iteh.ai/catalog/standards/sist/b84769a5-4e06-4d09-b9ce-d39e3cf6805b/iso-8730-1990

6.8.2 Extraction des éléments de message

Les règles d'extraction décrites en 6.6.2 doivent être appliquées.

6.8.3 Mise en page

Les règles de mise en page décrites en 6.7.2 doivent être appliquées.

6.9 Erreurs sur le code d'authentification du message (MAC)

6.9.1 Incapacité à générer un MAC

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, au minimum, pouvoir être constatée de façon lisible (par exemple, sur papier, écran ou microfiche, l'échec de l'opération doit être signalé par huit espaces (si possible) répartis en deux groupes de quatre, séparés par un caractère autre qu'un chiffre hexadécimal, de préférence un astérisque, par exemple, bbbb*bbbb. Lorsque des espaces ne sont pas disponibles, ils doivent être remplacés par des zéros; (par exemple, 0000*0000).