NORME INTERNATIONALE

ISO/CEI 10181-2

Première édition
1996-05-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre d'authentification

Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework

Numéro de référence
ISO/CEI 10181-2:1996(F)

Sommaire

Version française tirée en 1997

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement des Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10181-2 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information,* sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.811.

ISO/CEI 10181 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts*:

— *Partie 1: Aperçu*

— *Partie 2: Cadre d'authentification*

— *Partie 3: Cadre de contrôle d'accès*

— *Partie 4: Cadre de non-répudiation*

— *Partie 5: Cadre de confidentialité*

— *Partie 6: Cadre d'intégrité*

— *Partie 7: Cadre pour l'audit de sécurité et les alarmes*

Les annexes A à G de la présente partie de l'ISO/CEI 10181 sont données uniquement à titre d'information.

Introduction

Un grand nombre d'applications ont besoin de se sécuriser contre les menaces pesant sur la communication des informations. La Rec. X.800 du CCITT | ISO 7498-2 décrit les risques les plus courants ainsi que les services et les mécanismes qui peuvent être utilisés pour assurer une protection contre ces risques.

Les besoins en sécurité de nombreuses applications des systèmes ouverts sont liés à une identification correcte des entités principales impliquées. Ces besoins peuvent inclure la protection des biens et des ressources contre un accès non autorisé; dans ce cas, un mécanisme de contrôle d'accès fondé sur l'identité pourrait être utilisé. Il peut s'agir aussi de la mise en vigueur de responsabilités par la tenue de journaux d'audit où sont consignés des événements appropriés aussi bien que des informations comptables ou de taxation.

Le processus de confirmation d'identité est appelé authentification (ou légitimation). La présente Recommandation | Norme internationale définit un cadre général pour la fourniture de services d'authentification.

Page blanche

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE D'AUTHENTIFICATION

1 Domaine d'application

La série de Recommandations I Normes internationales sur les cadres de sécurité pour systèmes ouverts concerne l'application de services de sécurité dans un environnement de systèmes ouverts. Dans ce contexte, le terme «systèmes ouverts» recouvre les domaines tels que bases de données, applications réparties, traitement réparti ouvert et OSI. Les cadres de sécurité pour systèmes ouverts définissent les moyens de protection applicables aux systèmes et aux objets qu'ils contiennent. Ils traitent également des interactions entre les systèmes. Ils ne traitent pas de la méthode relative à la création de systèmes ou de mécanismes.

Les cadres de sécurité traitent à la fois des éléments de données et des séquences d'opérations (à l'exception des éléments de protocoles) utilisés pour obtenir des services de sécurité spécifiques. Ces services de sécurité peuvent s'appliquer aux entités de communication des systèmes et aux données échangées entre les systèmes ou gérées par eux.

La présente Recommandation I Norme internationale:

- définit les concepts de base relatifs à l'authentification;
- identifie les différentes classes de mécanismes d'authentification;
- définit les services correspondant à ces classes;

- identifie les spécifications fonctionnelles des protocoles supportant ces mécanismes;
- précise les spécifications générales de gestion pour les services d'authentification.

Différents types de normes peuvent utiliser ce cadre, par exemple:

1) les normes reprenant le concept d'authentification;
2) les normes relatives à la fourniture d'un service d'authentification;
3) les normes relatives à l'invocation d'un service d'authentification;
4) les normes spécifiant le moyen d'assurer l'authentification dans le cadre d'une architecture de système ouvert; et
5) les normes spécifiant des mécanismes d'authentification.

[A noter que les services mentionnés aux points 2), 3) et 4) peuvent comporter une authentification mais avoir un autre objet principal.]

Ces normes peuvent utiliser le présent Cadre comme suit:

- les normes des types 1), 2), 3), 4) et 5) peuvent utiliser la terminologie du présent Cadre;
- les normes des types 2), 3), 4) et 5) peuvent utiliser les services définis à l'article 7 du présent Cadre;
- les normes du type 5) peuvent être fondées sur les mécanismes définis à l'article 8 du présent Cadre.

A l'instar d'autres services de sécurité, l'authentification ne peut être assurée que dans le contexte d'une politique de sécurité définie pour une application donnée. La définition des politiques de sécurité ne relève pas du domaine d'application de la présente Recommandation I Norme internationale.

De même, la spécification détaillée des échanges protocolaires nécessaires à l'authentification ne fait pas partie du domaine de la présente Recommandation I Norme internationale.

La présente Recommandation I Norme internationale ne spécifie pas de mécanismes particuliers pour assurer des services d'authentification. D'autres normes (telle que l'ISO/CEI 9798) traitent plus en détail de méthodes d'authentification spécifiques et certaines d'entre elles (telle que la Rec. UIT-T X.509 I ISO/CEI 9594-8) exposent des exemples de méthodes se rapportant à des besoins d'authentification particuliers.

Certaines des procédures décrites ci-après réalisent la sécurité en appliquant des techniques cryptographiques. Toutefois, le présent Cadre ne repose pas sur l'utilisation d'un algorithme cryptographique donné ou d'une autre nature, bien que certaines classes de mécanismes d'authentification puissent dépendre de propriétés algorithmiques particulières, par exemple des propriétés asymétriques.

NOTE – L'ISO, bien que ne normalisant pas les algorithmes cryptographiques, normalise en fait les procédures utilisées pour les faire enregistrer dans l'ISO/CEI 9979.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation I Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation et Norme sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation I Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations I Normes internationales identiques

– Recommandation X.810[1] I ISO/CEI 10181-1:...[1], *Technologies de l'information – Cadres de sécurité pour les systèmes ouverts – Aperçu général.*

2.2 Paires de Recommandations I Normes internationales équivalentes par leur contenu technique

– Recommandation X.800 du CCITT: (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

2.3 Autres références

– ISO/CEI 9979:1991, *Techniques cryptographiques – Procédures pour l'enregistrement des algorithmes cryptographiques.*

– ISO/CEI 10116:1991, *Technologies de l'information – Modes opératoires d'un algorithme de chiffrement par blocs de n-bits.*

3 Définitions

La présente Recommandation I Norme internationale utilise les termes généraux suivants relatifs à la sécurité définis dans la Rec. X.800 du CCITT I ISO 7498-2:

– audit;
– enregistrement d'audit;
– informations d'authentification;
– confidentialité;
– cryptographie;
– valeur de contrôle cryptographique;
– authentification de l'origine des données;

---

[1] Actuellement à l'état de projet.

- intégrité des données;
- déchiffrement;
- signature numérique;
- chiffrement;
- clé;
- gestion de clés;
- usurpation d'identité;
- mot de passe;
- authentification de l'entité homologue;
- politique de sécurité.

La présente Recommandation | Norme internationale utilise le terme suivant, défini dans l'ISO/CEI 10116:

- chaînage de blocs.

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.810 | ISO/CEI 10181-1:

- empreinte numérique;
- fonction de hachage;
- fonction unidirectionnelle;
- clé privée;
- clé publique;
- scellé;
- clé secrète;
- autorité de sécurité;
- certificat de sécurité;
- domaine de sécurité;
- jeton de sécurité;
- confiance;
- tierce partie de confiance.

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent:

3.1 **méthode d'authentification asymétrique**: méthode d'authentification dans laquelle toutes les informations d'authentification ne sont pas partagées par les deux entités.

3.2 **identité authentifiée**: identificateur distinctif d'entité principale qui a été attesté par une authentification.

3.3 **authentification**: attestation de l'identité revendiquée par une entité.

3.4 **certificat d'authentification**: certificat de sécurité qui est garanti par une autorité d'authentification et qui peut être utilisé pour attester l'identité d'une entité.

3.5 **échange pour authentification**: séquence d'un ou de plusieurs transferts d'informations d'authentification (AI) pour échange, en vue de réaliser une authentification.

3.6 **informations d'authentification** (*authentication information*): renseignements utilisés aux fins de l'authentification.

3.7 **initiateur d'authentification**: entité qui commence l'échange pour authentification.

3.8 **épreuve**: paramètre variable dans le temps produit par un vérificateur.

3.9 **informations d'authentification pour déclaration (informations AI pour déclaration)**: informations utilisées par un déclarant pour produire les informations AI pour échange nécessaires à l'authentification d'une entité principale.

3.10 déclarant: entité qui est ou représente une entité principale à des fins d'authentification. Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

3.11 identificateur distinctif: information qui différencie sans ambiguïté une entité dans le processus d'authentification. La présente Recommandation I Norme internationale requiert qu'un identificateur de ce type soit non ambigu au moins dans un domaine de sécurité donné.

3.12 informations d'authentification pour échange (informations AI pour échange): informations échangées entre un déclarant et un vérificateur au cours du processus d'authentification d'une entité principale.

3.13 certificat d'authentification hors ligne: certificat d'authentification mis à la disposition de toutes les entités, qui associe un identificateur distinctif à des informations AI de vérification.

3.14 certificat d'authentification en ligne: certificat d'authentification utilisable dans un échange pour authentification, qui est obtenu directement par le déclarant auprès de l'autorité qui le garantit.

3.15 entité principale: entité dont l'identité peut être authentifiée.

3.16 méthode d'authentification symétrique: méthode dans laquelle les deux entités partagent des informations d'authentification communes.

3.17 paramètre variable dans le temps: élément de données utilisé par une entité pour vérifier qu'un message n'est pas une réexécution.

3.18 numéro unique: paramètre variable dans le temps, qui est produit par un déclarant.

3.19 informations d'authentification pour vérification (informations AI pour vérification): informations utilisées par le vérificateur pour vérifier une identité déclarée au moyen d'informations AI pour échange.

3.20 vérificateur: entité qui est ou qui représente l'entité revendiquant une identité authentifiée. Un vérificateur comporte les fonctions nécessaires pour engager des échanges pour authentification.

4 Abréviations

Pour les besoins de la présente Recommandation I Norme internationale, les abréviations suivantes sont utilisées.

AI Informations d'authentification (*authentification information*)

OSI Interconnexion des systèmes ouverts (*open systems interconnection*)

5 Présentation générale de l'authentification

5.1 Concepts de base relatifs à l'authentification

L'authentification donne l'assurance de l'identité revendiquée par une entité. Elle n'a de sens que dans un certain contexte. Deux cas importants se présentent:

- le contexte d'une relation de communication entre une entité principale et un vérificateur (authentification d'entité);
- le contexte d'une entité principale déclarant être à l'origine d'un élément de données mis à la disposition d'une autre entité (authentification d'origine des données).

La présente Recommandation I Norme internationale distingue deux formes particulières d'authentification.

L'authentification d'entité assure la corroboration de l'identité d'une entité principale, dans le contexte d'une relation de communication. L'identité authentifiée de cette entité principale n'est garantie que lorsque ce service est invoqué. On peut obtenir la garantie de la continuité d'authentification en suivant la description du 5.2.7. L'authentification d'une entité homologue OSI selon la Rec. X.800 du CCITT I ISO 7498-2 en est un exemple.

L'authentification d'origine de données assure la corroboration de l'identité de l'entité principale qui est responsable d'une unité de données spécifique.

NOTES

1 Lorsque l'on utilise le mode d'authentification d'origine de données, il faut également avoir une assurance suffisante du fait que les données n'ont pas été modifiées. Cela peut être accompli par un des moyens suivants:

a) par l'utilisation d'environnements dans lesquels les données ne puissent pas être altérées;

b) par la vérification du fait que les données reçues correspondent à une empreinte numérique des données envoyées;

c) par la fourniture de l'authentification d'origine des données au moyen d'un mécanisme de signature numérique;

d) par l'utilisation d'un algorithme cryptographique symétrique.

2 Le terme relation de communication, utilisé pour définir l'authentification d'entité, peut être interprété dans le sens large et désigner, par exemple, une connexion OSI, une communication entre processus ou une interaction entre un utilisateur et un terminal.

5.1.1 Identification et authentification

Une entité principale est une entité dont l'identité peut être authentifiée. Un ou plusieurs identificateurs distinctifs sont associés à une entité principale. Des services d'authentification peuvent être utilisés par des entités pour vérifier les entités déclarées par des entités principales. Une identité vérifiée de cette manière est appelée identité authentifiée.

Exemples d'entités principales pouvant être identifiées et, par conséquent, authentifiées:

- usagers;
- processus;
- systèmes ouverts réels;
- entités de couche OSI;
- entreprises.

Les identificateurs distinctifs doivent être non ambigus dans un domaine de sécurité donné. Ils différencient l'entité principale des autres entités de ce domaine au moyen de l'une des deux méthodes suivantes:

- à un degré de granularité peu discriminateur, par le fait que l'entité appartient à un groupe d'entités considérées comme équivalentes à des fins d'authentification (dans ce cas, les membres du groupe partagent le même identificateur distinctif); ou
- au degré de granularité le plus fin, en identifiant une seule et même entité.

Lorsque l'authentification s'effectue entre différents domaines de sécurité, il est possible qu'un identificateur distinctif ne suffise pas pour identifier sans ambiguïté une entité, car les autorités des différents domaines peuvent utiliser les mêmes identificateurs distinctifs. Dans ce cas, pour ne plus être ambigus, les identificateurs distinctifs doivent être associés à un identificateur de domaine de sécurité.

Parmi les identificateurs distinctifs les plus usités, figurent:

- les noms d'annuaires (Rec. UIT-T X.509 | ISO/CEI 9594-8);
- les adresses de couche réseau (Rec. UIT-T X.213 | ISO/CEI 8348);
- les titres de processus et d'entité d'application (Rec. UIT-T X.207 | ISO/CEI 9545);
- les identificateurs d'objets (Rec. UIT-T X.208 | ISO/CEI 8824);
- les noms de personnes (non ambigus dans le contexte du domaine);
- les numéros de passeport ou de sécurité sociale.

5.1.2 Entités d'authentification

Le terme déclarant désigne l'entité qui est ou qui représente une entité principale à des fins d'authentification. Un déclarant comporte des fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

Le terme vérificateur désigne l'entité qui est ou qui représente l'entité revendiquant une identité authentifiée. Un vérificateur comporte les fonctions nécessaires pour engager des échanges pour authentification.

Une entité engagée dans une authentification mutuelle (voir 5.2.4) prendra à la fois le rôle de déclarant et celui de vérificateur.

Le terme tiers caution désigne une autorité de sécurité, ou son agent, à laquelle d'autres entités accordent leur confiance en matière d'activités relatives à la sécurité. Dans le contexte de la présente Recommandation | Norme internationale, un tiers caution a la confiance d'un déclarant et/ou d'un vérificateur, à des fins d'authentification.

NOTE – Le déclarant ou le vérificateur peuvent être séparés en diverses composantes fonctionnelles, résidant éventuellement sur des systèmes ouverts distincts.

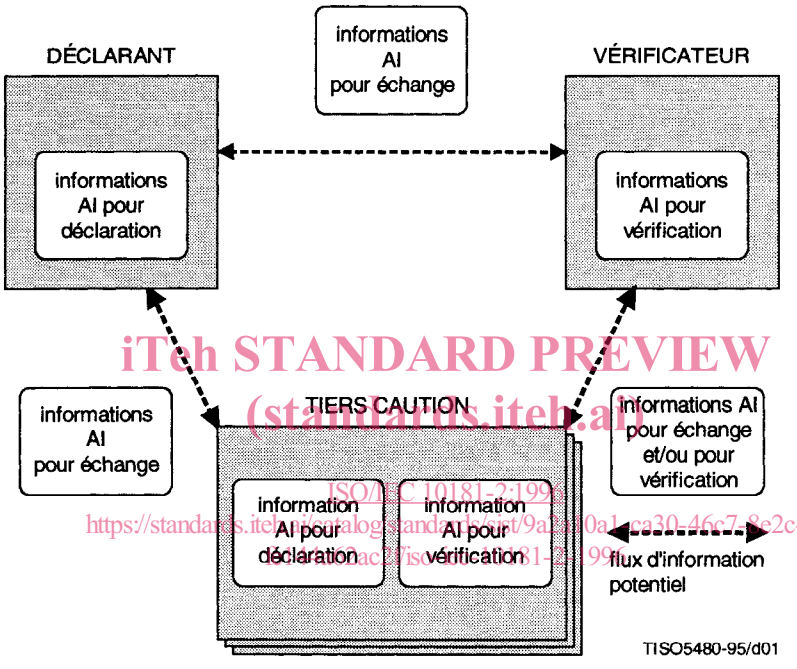
5.1.3 Informations d'authentification

Les types d'informations d'authentification sont les suivants:

- informations d'authentification pour échange (informations AI pour échange);
- informations d'authentification pour déclaration (informations AI pour déclaration);
- informations d'authentification pour vérification (informations AI pour vérification).

Le terme échange pour authentification désigne une série d'un ou de plusieurs transferts d'informations AI pour échange en vue d'exécuter une authentification.

La Figure 1 représente les relations entre le déclarant, le vérificateur, le tiers caution, ainsi que les trois types d'informations d'authentification.



NOTES

1 Dans certains scénarios, aucun tiers caution n'est impliqué.

2 Les informations AI pour vérification indiquées dans la Figure 1 peuvent être celles de l'entité principale ou celles du tiers caution (voir 5.5 pour de plus amples explications).

Figure 1 – Exemple de relations entre le déclarant, le vérificateur, le tiers caution, et types d'informations d'authentification

Dans certains cas, pour produire des informations AI pour échange, un déclarant peut avoir besoin d'interagir avec un tiers caution. De même, pour vérifier des informations AI pour échange, un vérificateur peut avoir besoin d'interagir avec un tiers caution. Dans ces cas, le tiers caution peut détenir des informations AI pour vérification se rapportant à une entité principale.

Il est également possible d'utiliser un tiers caution pour le transfert d'informations AI pour échange.

Les entités peuvent aussi avoir besoin de détenir des informations d'authentification qui serviront lors de l'authentification du tiers caution.

Le paragraphe 6.1 donne des exemples des trois types d'informations d'authentification.

NOTE – Le terme justificatif d'identité n'étant pas toujours employé de manière cohérente dans d'autres Recommandations I Normes internationales, le présent Cadre de sécurité ne l'utilise pas. Tel qu'il est défini dans la Rec. X.800 du CCITT I ISO 7498-2, le justificatif d'identité peut être un exemple d'informations AI pour échange.

5.2 Aspects des services d'authentification

5.2.1 Risques pour l'authentification

L'authentification a pour but d'attester l'identité d'une entité principale. Les mécanismes d'authentification doivent normalement éliminer les risques d'usurpation et de réexécution.

L'usurpation d'identité est le procédé par lequel une entité se fait passer pour une autre. C'est-à-dire que l'entité prétend être une autre entité qui est en relation spécifique avec le vérificateur (par exemple dans le cadre d'une authentification d'origine de données ou dans celui d'une relation de communication). Ces types de risques sont la réexécution, le relais et la compromission d'informations AI pour déclaration.

Un risque d'usurpation d'identité apparaît au cours d'une activité (par exemple dans le cadre d'une authentification d'origine de données ou dans celui d'une relation de communication) lancée soit par le déclarant ou par le vérificateur. La protection contre les risques encourus par une activité à cause d'une usurpation d'identité dépend de l'association existant entre le mécanisme d'authentification et cette activité. Pour contrer les risques associés à l'usurpation d'identité, l'authentification doit toujours être utilisée en combinaison avec une forme de service d'intégrité qui associe l'identité authentifiée à l'activité.

La réexécution consiste à répéter des informations AI pour échange afin d'obtenir un effet non autorisé. Cette attaque est généralement utilisée conjointement avec d'autres, comme la modification de données. Les méthodes d'authentification ont une efficacité inégale contre la réexécution. La réexécution peut constituer un risque pour d'autres services de sécurité. L'authentification peut être utilisée pour contrer la réexécution car elle offre le moyen de déterminer l'origine des informations échangées.

5.2.2 Transmission d'authentification

Dans certaines circonstances, une entité principale peut devoir agir indirectement dans un système. Dans ce cas, il faudra créer une représentation de l'entité principale dans le système et, auparavant, authentifier l'entité principale.

Lorsqu'un agent agit au nom de l'entité principale, la représentation de cet agent sera authentifiée à la place de celle de l'entité principale. Etant donné que la représentation se comporte comme si elle était l'entité principale, les actions de cette dernière peuvent être exécutées à l'intérieur du système sans que l'entité principale soit impliquée directement. Un exemple de ce cas de figure est présenté dans l'Annexe A.

Outre le fait que l'on peut avoir des représentations possédant une durée de vie indépendante, dans le cas où l'entité principale est un usager, il est possible d'utiliser des représentations avec des mécanismes qui lient la durée de vie de la représentation à la présence de l'usager.

Un déclarant agissant au nom de l'entité principale peut accéder à un autre système qui crée sa propre représentation de l'entité principale après l'authentification. La création de cette représentation est appelée transmission d'authentification.

La possibilité de transmettre ainsi l'authentification peut dépendre de la politique de sécurité.

5.2.4 Authentification unilatérale et mutuelle

L'authentification peut être unilatérale ou mutuelle. La première atteste l'identité d'une seule entité principale. La seconde atteste l'identité des deux entités principales.

L'authentification d'entité peut être soit mutuelle, soit unilatérale. Par nature, l'authentification d'origine de données est toujours unilatérale.

5.2.5 Lancement d'un échange pour authentification

Un échange pour authentification peut être lancé par le déclarant ou par le vérificateur. L'entité qui commence l'échange est appelée initiateur d'authentification.

5.2.6 Révocation d'informations d'authentification

La révocation d'informations d'authentification se rapporte à l'invalidation permanente d'informations AI pour vérification.

Dans certaines situations, la politique de sécurité peut exiger la révocation d'informations d'authentification. Cette décision peut être justifiée par la détection de cas de violation de la sécurité, par une modification de politique ou par d'autres raisons. Elle peut entraîner ou non la révocation des accès existants ou avoir d'autres effets connexes.

Les opérations de gestion ci-après peuvent en outre être engagées:

a) enregistrement de l'événement dans le journal d'audit;

b) notification locale de l'événement;

c) notification à distance de l'événement; et/ou

d) déconnexion d'une relation de communication.

L'action à mener en fonction de chaque événement dépend de la politique de sécurité en vigueur, ainsi que d'autres facteurs liés à l'état de la communication, par exemple si une mise à jour a eu lieu pendant que l'entité principale était connectée et active.

5.2.7 Garantie de la continuité de l'authentification

L'authentification d'entité ne garantit une identité qu'à un moment donné. Un moyen d'obtenir la garantie de continuité de l'authentification consiste à établir un lien entre le service d'authentification et le service d'intégrité de données.

Un service d'authentification et un service d'intégrité sont réputés être liés si l'entité principale est authentifiée initialement par un service d'authentification et si ce service, ainsi que les informations qui lui seront liées ultérieurement, font appel à un service d'intégrité. Cela garantit que les informations ultérieures ne pourront pas être altérées par une autre entité quelconque et qu'elles ne pourront donc venir que de l'entité principale authentifiée initialement. Il importe que le service d'intégrité soit assuré sur l'ensemble du trajet suivi par les informations entre l'entité principale et le vérificateur. Une usurpation d'identité est par exemple possible si certaines des informations peuvent être produites par des entités principales autres que celle qui a été authentifiée.

Une autre manière d'obtenir la garantie que la même entité distante est encore présente un peu plus tard consiste à effectuer de temps en temps d'autres échanges d'informations d'authentification. Mais cela n'empêchera pas des intrusions pendant les intervalles, ce qui fait qu'aucune garantie de continuité ne peut être donnée. L'attaque suivante est par exemple possible: un intrus, au moment où il lui est demandé de continuer l'authentification, laisse le tiers autorisé effectuer les opérations correspondantes puis reprend le contrôle.

Si le mécanisme d'intégrité requiert une clé, celle-ci peut être dérivée de paramètres spécifiés lors de l'échange pour authentification. Une fois établie l'association entre cette clé et l'entité principale authentifiée, le mécanisme d'intégrité s'en servira pour lier comme décrit ci-dessus les deux services fournis.

La manière de dériver une clé pour un service d'intégrité peut être spécifiée dans le cadre des paramètres spécifiant les méthodes et les algorithmes à utiliser pour l'échange pour authentification.

NOTE – Lorsque d'autres services de sécurité sont utilisés, il est également possible de dériver des informations de service à partir des paramètres spécifiés au cours de l'échange pour authentification, par exemple à partir d'une clé de confidentialité.

5.2.8 Répartition des composantes d'authentification entre de multiples domaines

Les domaines de sécurité peuvent avoir des relations telles que le déclarant d'un domaine puisse être authentifié par le vérificateur d'un autre domaine. De multiples domaines de sécurité peuvent intervenir, notamment:

- le domaine de sécurité dans lequel réside l'initiateur;
- le domaine de sécurité dans lequel réside le vérificateur;
- le domaine de sécurité dans lequel réside le tiers caution.

Il n'est pas nécessaire que ces domaines soient distincts.

Avant d'effectuer une authentification entre différents domaines de sécurité, il est nécessaire de définir une politique de sûreté interactive.

5.3 Principes d'authentification

En général, chaque méthode d'authentification repose sur un ensemble d'hypothèses ou de prévisions liées à un ou plusieurs principes.

Ces principes sont les suivants:

a) la connaissance de quelque chose (par exemple d'un mot de passe);

b) la possession de quelque chose (par exemple d'une carte magnétique ou à puce);

c) une caractéristique immuable (par exemple des identifiants biométriques);

d) l'acceptation du fait qu'une tierce partie (le tiers caution) a établi l'authentification;

e) le contexte (par exemple l'adresse de l'entité principale).

Il convient de noter que tous ces principes ont leurs points faibles intrinsèques. Par exemple, l'authentification par possession consiste le plus souvent à authentifier l'objet possédé plutôt que son possesseur. Dans certains cas, on peut pallier le point faible en associant plusieurs principes. Par exemple, en cas d'utilisation d'une carte à puce (qui est quelque chose que l'on possède), on peut pallier le point faible en ajoutant un numéro d'identification personnel (PIN) (qui est quelque chose dont on doit avoir connaissance) afin de légitimer l'utilisateur de la carte. Par ailleurs, le principe e) est particulièrement vulnérable et est presque toujours utilisé conjointement avec un autre principe.

Il y a lieu de noter, s'agissant du principe d), qu'il existe deux types de récurrence:

- pour être identifiée, l'entité tierce pourrait elle-même avoir à être authentifiée;
- l'authentification établie par l'entité tierce peut impliquer l'intervention d'une quatrième entité, etc.

L'analyse des méthodes d'authentification réelles qui prennent en compte ces principes donnera des indications quant aux entités impliquées, aux principes utilisés et aux entités principales authentifiées.

5.4 Phases d'authentification

Les procédures d'authentification peuvent comporter les phases suivantes:

- installation;
- modification des informations d'authentification;
- distribution;
- acquisition;
- transfert;
- vérification;
- désactivation;
- réactivation;
- désinstallation.

Les phases décrites ici ne sont pas obligatoirement séparées dans le temps; elles peuvent se chevaucher.

Un schéma d'authentification donné ne requiert pas nécessairement toutes ces phases. Il est également possible que l'enchaînement des phases varie par rapport à l'ordre dans lequel elles sont décrites ci-dessous.

5.4.1 Installation

Lors de la phase d'installation, on définira les informations AI pour déclaration et les informations AI pour vérification.

5.4.2 Modification des informations d'authentification

Lors de la phase de modification des informations d'authentification, une entité principale ou un gestionnaire modifie les informations AI pour déclaration et les informations AI pour vérification (par exemple modification d'un mot de passe).

5.4.3 Distribution

Lors de la phase de distribution, des informations AI pour vérification sont distribuées à une entité (par exemple, un déclarant ou un vérificateur) afin de vérifier des informations AI pour échange. Par exemple, dans les processus d'authentification hors ligne, des entités peuvent obtenir des certificats d'authentification, des listes de révocation de certificats et des listes de révocation d'autorités. La phase de distribution peut être antérieure, coïncidente ou postérieure à la phase de transfert.