UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

# UIT-T X.811

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(04/95)

## RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

## SÉCURITÉ

---

# TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS CADRES DE SÉCURITÉ POUR SYSTÈMES OUVERTS: CADRE D'AUTHENTIFICATION

## Recommandation UIT-T X.811

(Antérieurement «Recommandation du CCITT»)

---

## AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution nº 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI. Le texte de la Recommandation X.811 de l'UIT-T a été approuvé le 10 avril 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-2.

---

NOTE

Dans la présente Recommandation, l'expression «Administration» est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS**

(Février 1994)

**ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X**

| Domaine | Recommandations |
|---|---|
| RÉSEAUX PUBLICS POUR DONNÉES | |
| Services et services complémentaires | X.1-X.19 |
| Interfaces | X.20-X.49 |
| Transmission, signalisation et commutation | X.50-X.89 |
| Aspects réseau | X.90-X.149 |
| Maintenance | X.150-X.179 |
| Dispositions administratives | X.180-X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | |
| Modèle et notation | X.200-X.209 |
| Définition des services | X.210-X.219 |
| Spécifications des protocoles en mode connexion | X.220-X.229 |
| Spécifications des protocoles en mode sans connexion | X.230-X.239 |
| Formulaires PICS | X.240-X.259 |
| Identification des protocoles | X.260-X.269 |
| Protocoles de sécurité | X.270-X.279 |
| Objets gérés de couche | X.280-X.289 |
| Test de conformité | X.290-X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | |
| Considérations générales | X.300-X.349 |
| Systèmes mobiles de transmission de données | X.350-X.369 |
| Gestion | X.370-X.399 |
| SYSTÈMES DE MESSAGERIE | X.400-X.499 |
| ANNUAIRE | X.500-X.599 |
| RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES | |
| Réseautage | X.600-X.649 |
| Dénomination, adressage et enregistrement | X.650-X.679 |
| Notation de syntaxe abstraite numéro un (ASN.1) | X.680-X.699 |
| GESTION OSI | X.700-X.799 |
| SÉCURITÉ | X.800-X.849 |
| APPLICATIONS OSI | |
| Engagement, concomitance et rétablissement | X.850-X.859 |
| Traitement des transactions | X.860-X.879 |
| Opérations distantes | X.880-X.899 |
| TRAITEMENT OUVERT RÉPARTI | X.900-X.999 |

# TABLE DES MATIÈRES

## 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.

**NORME INTERNATIONALE**

**RECOMMANDATION UIT-T**

# TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITE POUR SYSTÈMES OUVERTS: CADRE D'AUTHENTIFICATION

## 1 Domaine d'application

La série de Recommandations | 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 | 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 | Norme internationale.

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

La présente Recommandation | 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 | 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 | 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 | 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 | Normes internationales identiques

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

### 2.2 Paires de Recommandations | 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 | Norme internationale utilise les termes généraux suivants relatifs à la sécurité définis dans la Rec. X.800 du CCITT | 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 | 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 | 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 | 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 | 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.

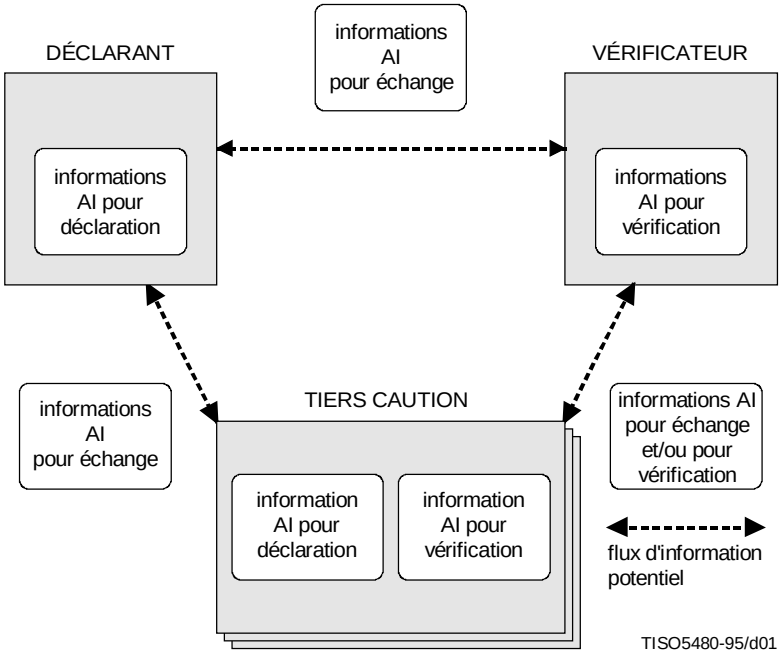
### 5.1.3 Informations d'authentification

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 | Normes internationales, le présent Cadre de sécurité ne l'utilise pas. Tel qu'il est défini dans la Rec. X.800 du CCITT | 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.

#### 5.4.4 Acquisition

Dans la phase d'acquisition, un déclarant ou un vérificateur peut obtenir les informations nécessaires pour produire des informations AI pour échange spécifiques dans une instance d'authentification donnée. Diverses procédures permettent l'acquisition d'informations AI pour échange par interaction avec un tiers caution ou par échange de messages entre les entités effectuant l'authentification.

Par exemple, lorsqu'ils utilisent un centre de distribution de clés directes, le déclarant ou le vérificateur peuvent obtenir de ce centre certaines informations, telles qu'un certificat d'authentification (voir 6.1.3), qui permettent l'authentification avec l'autre entité.

#### 5.4.5 Transfert

Lors de la phase de transfert, des informations AI pour échange sont transférées entre le déclarant et le vérificateur.

#### 5.4.6 Vérification

Lors de la phase de vérification, les informations AI pour échange sont comparées aux informations AI pour vérification. Dans cette phase, une entité qui ne peut pas vérifier elle-même les informations AI pour échange peut prendre contact avec un tiers caution qui effectuera la vérification des informations AI pour échange et enverra ensuite une réponse, négative ou positive.

#### 5.4.7 Désactivation

Lors de la phase de désactivation, un état est établi qui rend temporairement impossible l'authentification d'une entité principale précédemment authentifiable.

#### 5.4.8 Réactivation

Lors de la phase de réactivation, l'état établi lors de la phase de désactivation est annulé.

#### 5.4.9 Désinstallation

La phase de désinstallation consiste à enlever une entité principale d'un groupe d'entités principales.

### 5.5 Participation de tiers caution

Les mécanismes d'authentification peuvent être caractérisés par le nombre de tiers caution qu'ils impliquent.

#### 5.5.1 Authentification sans participation de tiers caution

Dans le plus simple des cas, ni le déclarant ni le vérificateur ne sont acceptés par une autre entité pour la production et la vérification d'informations AI pour échange. Dans ce cas, la phase de vérification d'informations AI pour l'entité principale doit déjà être installée dans le vérificateur.

Sauf si les entités n'ont qu'un nombre restreint de partenaires de communication possibles, cette approche est peu utilisée pour les environnements de communication à grande échelle. Dans le pire des cas, chaque vérificateur doit disposer des informations AI pour vérification de toutes les entités principales d'un domaine de sécurité; la quantité totale d'informations nécessaires correspond alors au carré du nombre d'entités mises en jeu.

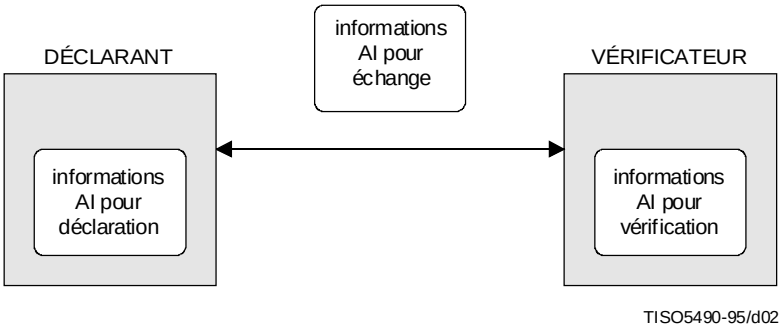



**Figure 2 – Authentification sans tiers caution**

### 5.5.2 Authentification avec participation de tiers caution

Une information AI peut être obtenue par interaction avec des tiers caution. L'intégrité de ces informations doit être garantie. Il est également nécessaire de maintenir la confidentialité des informations AI pour déclaration du tiers caution, ainsi que des informations AI pour vérification si l'on peut en dériver des informations AI pour déclaration.

L'authentification peut faire intervenir un tiers caution ou une chaîne de tiers caution selon le principe décrit en d) du 5.3. L'introduction de tiers caution supplémentaires permet d'étendre les opérations d'authentification à une nombreuse population d'entités, chaque tiers caution ne conservant des informations que sur un nombre limité d'entités (et non sur toutes). Le volume total d'informations peut ainsi augmenter de manière linéaire avec le nombre d'entités impliquées.

Les relations multientités peuvent être classées selon les conditions de la communication (nombre de liaisons actives mises en jeu) et selon le degré de contrôle de gestion qu'elles possèdent, par exemple le délai inhérent à la révocation d'informations d'authentification.

#### 5.5.2.1 Authentification en coupure de ligne

Dans ce type d'authentification, une entité caution (un intermédiaire) intervient directement dans un échange pour authentification entre le déclarant et le vérificateur. Une entité principale est authentifiée par l'intermédiaire qui alors se porte garant de l'identité dans l'échange pour authentification en coupure de ligne qui s'ensuit.

L'authentification en coupure de ligne suppose que le vérificateur fasse confiance à l'intermédiaire pour ce qui est de l'authentification de l'entité principale et que le vérificateur soit assuré de l'identité de l'intermédiaire par le biais d'une authentification.

La révocation de la capacité d'authentifier peut être réglée en fonction de la granularité de la prochaine tentative d'authentification. Si le déclarant constate une révocation de ses informations d'authentification, l'intermédiaire peut immédiatement mettre à jour le statut de ce déclarant et rejeter toutes tentatives d'authentification éventuellement reçues par la suite.

Parfois, l'authentification peut être étendue de manière à recevoir une garantie mettant en jeu une chaîne d'intermédiaires caution selon la politique de sécurité en vigueur, il incombe au vérificateur ou au dernier tiers caution de la chaîne de s'amuser de la validité de cette chaîne.

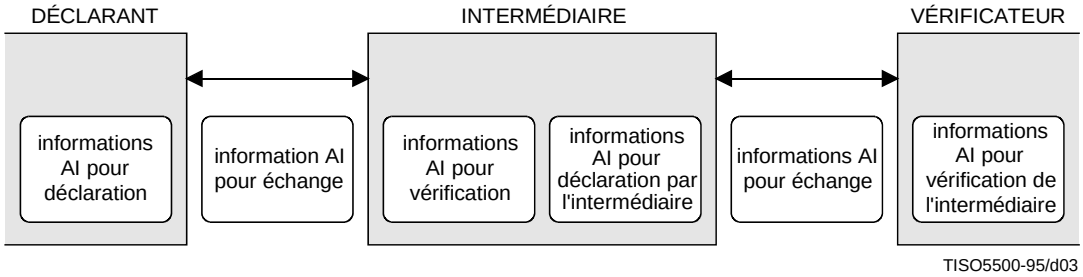



**Figure 3 – Authentification en coupure de ligne**

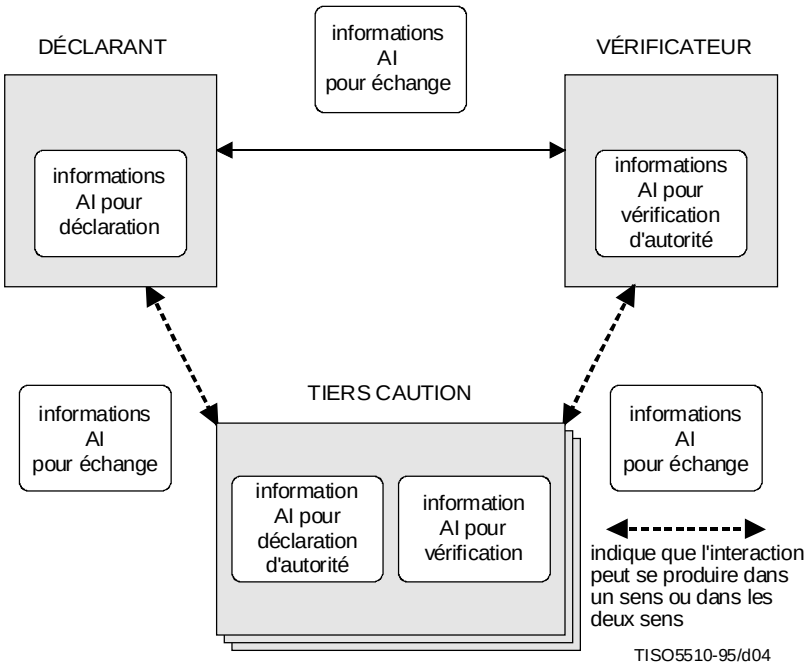
#### 5.5.2.2 Authentification en ligne

Dans ce type d'authentification, un ou plusieurs tiers caution interviennent activement à chaque instance d'un échange pour authentification. Toutefois, contrairement à ce qui se passe dans l'authentification en coupure de ligne, les tiers caution connectés ne se trouvent pas directement sur le trajet de l'échange pour authentification entre le déclarant et le vérificateur. Le déclarant peut faire appel aux tiers caution pour produire des informations AI pour échange et celles-ci peuvent aider le vérificateur dans sa vérification des informations AI pour échange. Un tiers caution connecté peut produire des certificats d'authentification en ligne (voir 6.1.3).

L'authentification en ligne suppose qu'une chaîne de tiers caution intervienne dans la production des informations AI pour échange entre le vérificateur et le tiers caution susceptible de valider les informations AI pour déclaration de l'entité principale. Dans le cas le plus simple, l'interaction directe d'un seul tiers caution est nécessaire avec le déclarant ou avec le vérificateur. L'interaction peut toutefois être étendue à une chaîne de tiers caution qui communiqueront directement ou indirectement avec le déclarant ou avec le vérificateur.

La révocation de la capacité d'authentifier peut être réglée en fonction de la granularité de la tentative d'authentification suivante.

Parmi les tiers caution en ligne, on trouve par exemple les serveurs d'authentification en ligne ou les centres de distribution de clés.




NOTE – Les informations AI pour échange transitant réellement entre les trois entités distinctes représentées sur cette figure ne sont pas les mêmes.

**Figure 4 – Authentification en ligne**

### 5.5.2.3 Authentification hors ligne

L'authentification hors ligne se caractérise par la nécessité de recourir à des listes certifiées de certificats révoqués, des listes de certificats, des certificats révoqués, aux délais d'expiration des certificats, ou à d'autres méthodes non immédiates de révocation de l'information AI de vérification.

Dans ce type d'authentification, un ou plusieurs tiers caution prennent en charge l'authentification sans être impliqués dans chaque instance d'authentification. Ces tiers produisent et distribuent à l'avance des certificats d'authentification non ligne que le vérificateur peut utiliser ensuite pour valider un échange pour authentification. L'échange se poursuit de manière autonome, sans l'intervention de l'autorité.

Les tiers caution n'ayant pas à interagir directement avec le déclarant ou avec le vérificateur au moment même de l'authentification, ce procédé peut être plus rentable si l'on considère le nombre d'interactions requises.

Des dispositions supplémentaires doivent être prévues pour la révocation, telles que temporisation et renouvellement des certificats, listes certifiées de certificats révoqués.

Parmi les tiers caution hors ligne, on trouve par exemple les autorités de certification qui délivrent les certificats d'authentification hors ligne (voir 6.1.3).

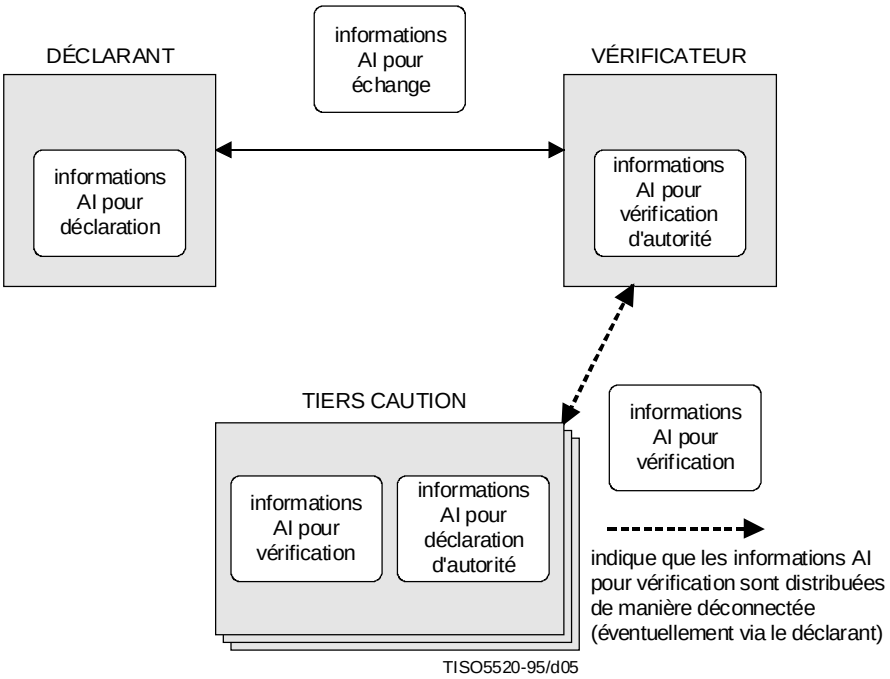



**Figure 5 – Authentification hors ligne**

### 5.5.3 Confiance du déclarant dans le vérificateur

Les mécanismes pour lesquels il est nécessaire d'avoir confiance en un vérificateur sont inadéquats, sauf lorsque la confiance peut être accordée à tous les vérificateurs possibles. En effet, si l'identité du vérificateur n'a pas été authentifiée, il est impossible de savoir s'il est digne de confiance. Par exemple, la simple utilisation d'un mot de passe pour l'authentification implique l'assurance qu'un vérificateur ne conservera pas le mot de passe pour le réutiliser par la suite.

## 5.6 Types d'entités principales

Les entités principales peuvent être classées selon différentes catégories. Par exemple:

a) entités à caractéristique(s) passives(s), par exemple empreintes digitales ou rétiniennes;

b) entités avec capacités de traitement et d'échange d'informations;

c) entités avec capacités de stockage d'informations;

d) entités à localisation fixe.

Certaines entités principales peuvent présenter plusieurs de ces aspects [par exemple une entité humaine possède les aspects a), b) et c)]. Chaque type d'aspects relève d'une méthode d'authentification différente:

a) mesure de caractéristique(s) passive(s);

b) épreuve complexe et évaluation des réponses;

c) mémorisation d'un secret (tel qu'un mot de passe);

d) détermination d'une localisation.

## 5.7 Authentification d'usagers

Dans une instance d'authentification, il peut être nécessaire d'identifier l'usager humain final, plutôt qu'un processus agissant au nom de cet usager.

Les méthodes d'authentification des usagers doivent être acceptables pour ces derniers, tout en restant économiques et efficaces. Le recours à des méthodes inacceptables peut inciter les usagers à trouver le moyen de contourner les procédures, augmentant ainsi les risques d'intrusion.

L'authentification d'usagers est généralement fondée sur les principes décrits en 5.3. Les procédures correspondantes sont fondées sur les phases décrites en 5.4.

L'Annexe A fournit des informations supplémentaires sur l'authentification d'usagers et sur les processus agissant au nom de ceux-ci.

## 5.8 Types d'attaque visant l'authentification

Trois formes d'attaque sont prises en considération:

- les *attaques par réexécution*, dans lesquelles des informations AI pour échange sont lues et réexécutées ultérieurement;
- les *attaques par relais* lancées par un intrus;
- les *attaques par relais* au cours desquelles un intrus répond.

Une attaque par relais se caractérise par le fait que des informations AI pour échange sont interceptées puis immédiatement réexécutées.

### 5.8.1 Attaques par réexécution

Deux cas de réexécution sont à prendre en compte. Il s'agit de la réexécution d'informations AI pour échange:

- destinées au même vérificateur; ou
- destinées à un autre vérificateur.

Ce dernier cas peut se produire lorsque les (mêmes) informations AI pour vérification d'une entité principale sont connues de plusieurs vérificateurs. Lorsqu'une réexécution peut réussir, il s'agit d'un cas particulier de l'usurpation d'identité.

Les deux types de réexécution peuvent être contrés par des épreuves. Celles-ci sont produites par le vérificateur. La même épreuve ne doit jamais être posée deux fois par le même vérificateur, ce qui peut être assuré de plusieurs manières (voir l'Annexe C).

#### 5.8.1.1 Réexécution destinée au même vérificateur

On peut contrer la réexécution destinée au même vérificateur en utilisant des numéros uniques ou des épreuves.

Les numéros uniques sont produits par le déclarant. Le même numéro unique ne doit jamais être accepté deux fois par le même vérificateur, ce qui peut être assuré de plusieurs manières (voir l'Annexe C).

#### 5.8.1.2 Réexécution destinée à un vérificateur différent

On peut contrer la réexécution destinée à un vérificateur différent en utilisant des épreuves. En variante, on peut utiliser, lors du calcul des informations AI pour échange, une caractéristique quelconque qui est unique pour le vérificateur. Une telle caractéristique peut être le nom du vérificateur, son adresse de couche réseau ou généralement tout attribut en relation biunivoque avec les vérificateurs qui se partagent les mêmes informations AI pour vérification.

### 5.8.2 Attaques par relais

#### 5.8.2.1 Attaques par relais lancées par un intrus

Ce type d'attaque suppose que l'intrus est l'initiateur de l'authentification. Cette attaque n'est possible que si le déclarant et le vérificateur sont tous les deux en mesure de lancer l'authentification. Cette attaque fait que, sans le savoir, le déclarant et le vérificateur échangent des informations d'authentification via un intrus; c'est-à-dire que celui-ci se fait passer pour un certain vérificateur à l'égard d'un déclarant et pour ce déclarant à l'égard de ce vérificateur.

Par exemple, supposons que l'intrus C veut se faire passer, auprès du vérificateur B, pour le déclarant A. L'intrus C lance une interaction avec les entités A et B. C informe A qu'il est B et demande à A de se légitimer auprès de B, tout en informant B qu'il est A et qu'il désire se légitimer (voir la Figure 6).

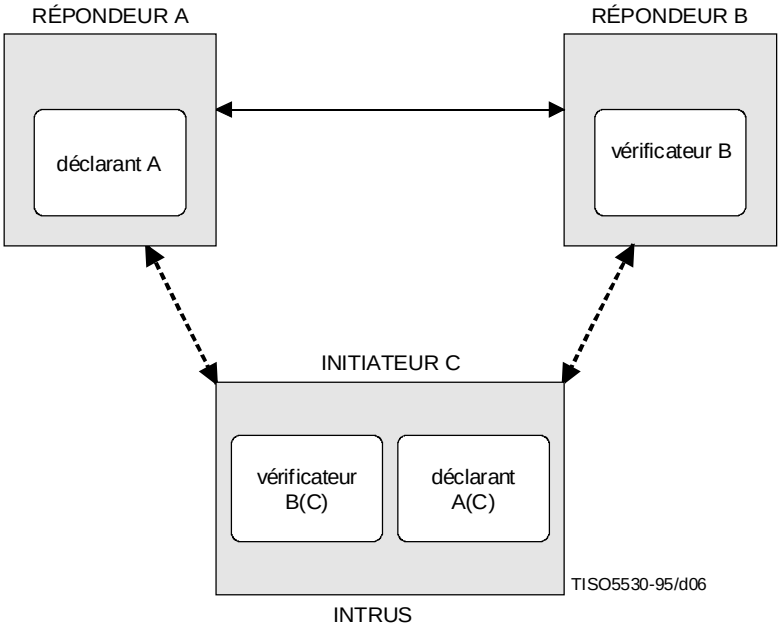



**Figure 6 – Attaque par relais lancée par intrus**

Au cours du processus d'authentification, l'entité A joue le rôle de déclarant auprès de B (en fait auprès de C se faisant passer pour B) et fournit donc des informations dont l'entité C peut se servir pour se légitimer auprès de B. Celui-ci joue le rôle de vérificateur et fournit également les informations dont C a besoin pour jouer le rôle de vérificateur. A la suite de l'authentification, l'intrus C apparaîtra à B comme étant l'entité A authentifiée.

On peut contrer ce type d'attaque si:

a) l'entité qui lance une interaction est toujours le déclarant ou toujours le vérificateur (à noter que cela n'est pas possible en cas d'authentification mutuelle); ou

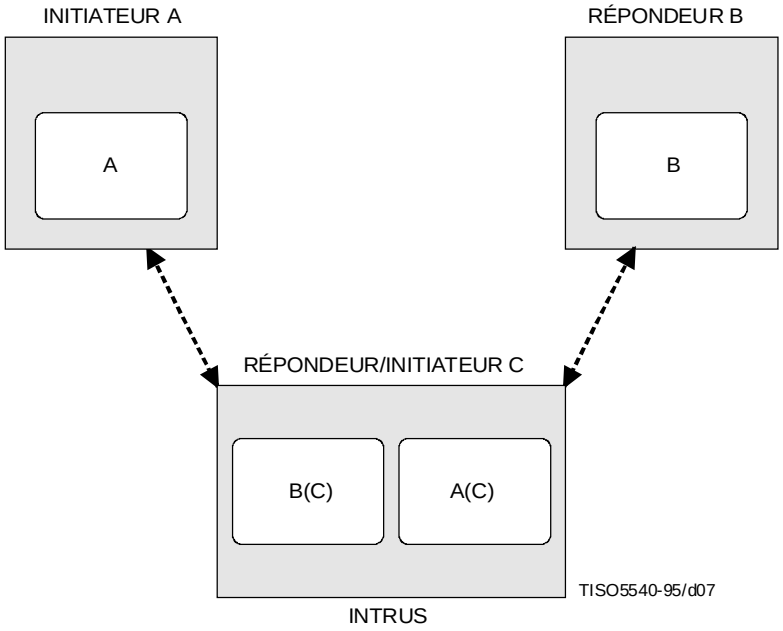
b) si les informations AI pour échange fournies par le déclarant sont différentes selon qu'il joue le rôle d'initiateur d'une demande d'authentification ou celui de répondeur à une invitation à s'authentifier. Cette différence permet au vérificateur de détecter l'interception décrite. Pour plus de détails, voir l'Annexe D.

#### 5.8.2.2 Attaques par relais avec réponse d'intrus

Dans ce type d'attaque, l'intrus s'immisce au milieu d'un échange pour authentification, intercepte les informations d'authentification et les renvoie en prenant le rôle de l'initiateur. Ce type d'attaque peut se produire soit de manière opportuniste (auquel cas l'intrus attend d'être pris par erreur pour le répondeur) ou de manière systématique (auquel cas l'intrus se targue d'être le répondeur, par exemple dans une table d'emplacements de ressources centrales).

La parade générale contre ce type d'attaque nécessite l'emploi d'un service complémentaire (d'intégrité ou de confidentialité). Les informations AI pour échange sont combinées avec d'autres informations permettant au déclarant et au vérificateur, à condition qu'ils soient les interlocuteurs légitimes, de calculer une clé. La clé calculée pourra ensuite être utilisée pour ouvrir un mécanisme d'intégrité ou de confidentialité à base cryptographique.

Une autre parade est possible lorsque le réseau de communication n'est pas soumis à des interceptions internes, c'est-à-dire lorsqu'il remet toujours à l'adresse correcte des données intactes. Dans cette situation, on peut contrer l'attaque en intégrant les adresses de réseau dans les informations AI pour échange (par exemple, en signant l'adresse de réseau).




NOTES

1 Même si les attaques lancées par intrus sont contrées au moyen des parades a) ou b) du 5.8.2.1, une méthode d'authentification restera vulnérable à une attaque avec réponse d'intrus.

2 La notation X(Y) indique que Y se fait passer pour X.

**Figure 7 – Attaque par relais avec réponse d'intrus**

# 6 Informations et services d'authentification

## 6.1 Informations d'authentification

### 6.1.1 Informations d'authentification pour déclaration (informations AI pour déclaration)

Les informations AI pour déclaration sont les informations utilisées en vue de produire les informations AI pour échange nécessaires à l'authentification de l'entité principale.

Des exemples d'informations AI pour déclaration sont les suivants:

a) *un mot de passe*;

b) *une clé secrète*, utilisée avec des mécanismes d'authentification à algorithmes de chiffrement symétriques;

c) *une clé privée*, utilisée avec des mécanismes d'authentification à algorithmes de chiffrement asymétriques.

### 6.1.2 Informations d'authentification pour vérification (informations AI pour vérification)

Les informations AI pour vérification servent à vérifier une identité déclarée par des informations AI pour échange.

Des exemples d'informations AI pour vérification sont les suivants:

a) *un mot de passe* associé à l'identité d'une entité principale;

b) *une clé secrète*, associée à l'identité d'une entité principale ou d'une autorité et utilisée avec des mécanismes d'authentification à algorithmes de chiffrement symétriques;

c) *une clé publique*, associée à l'identité d'une entité principale ou d'une autorité et utilisée avec des mécanismes d'authentification à algorithmes de chiffrement asymétriques.

Les informations AI pour vérification peuvent être fournies sous la forme d'une table d'authentification et/ou d'un certificat d'authentification hors ligne (voir 6.1.4.2).

Une table d'authentification est constituée d'un ensemble d'entrées directement accessibles par le vérificateur. Le trajet d'accès à une table est protégé par des mécanismes d'intégrité auxquels s'ajoute, dans le cas de mécanismes symétriques, la protection par confidentialité.

Une entrée de table d'authentification peut, par exemple, contenir les éléments suivants:

- identité de l'entité principale;
- information AI de vérification (mot de passe, clé secrète ou clé publique, par exemple);
- période de validité pour l'entrée;
- politique de sécurité applicable à l'entrée;
- autorité responsable de l'entrée.

### 6.1.3 Informations d'authentification pour échange (informations AI pour échange)

L'information AI d'échange est une information échangée par le déclarant et le vérificateur au cours du processus d'authentification d'une entité principale. Il s'agira par exemple:

- d'un identificateur distinctif déclaré;
- d'un mot de passe;
- d'une épreuve;
- d'une réponse à une épreuve;
- d'un numéro unique;
- d'un identificateur distinctif de vérificateur;
- du résultat de l'application d'une fonction de transformation à des informations AI pour déclaration ou à d'autres données, ou de l'utilisation par cette fonction d'informations AI pour déclaration ou d'autres données (par exemple horodatage, nombre aléatoire, compteur, épreuve, identité de vérificateur, empreinte numérique, identité de déclarant). On trouve parmi ces fonctions de transformation les fonctions univoques, la fonction de chiffrement asymétrique et la fonction de chiffrement symétrique;
- d'un certificat d'authentification en ligne;
- d'un certificat d'authentification hors ligne.

Tout ou partie des informations AI pour échange transmises au cours d'un même transfert peut l'être sous la forme d'un jeton de sécurité.

### 6.1.4 Certificats d’authentification

Le certificat d'authentification est une forme commune d'information d'authentification. Il s'agit d'un type particulier de certificat de sécurité, attesté par une autorité caution et pouvant être utilisé à des fins d'authentification.

Il existe différents types de certificats d'authentification:

- certificat d'authentification en ligne;
- certificat d'authentification hors ligne;
- certificat de révocation d'authentification;
- listes de certificats de révocation d'authentification.

Les certificats d'authentification hors ligne (voir 6.1.4.2) ne sont applicables qu'aux informations AI pour vérification liées aux clés publiques. Leur validité peut être annulée par le biais d'un certificat de révocation ou d'une table de révocation.

Les certificats d'authentification peuvent contenir, par exemple, les éléments suivants:

- identification de la méthode et/ou de la clé utilisées en vue de créer une valeur de contrôle cryptographique;
- identité de l'autorité d'authentification et identité de l'agent ayant délivré le certificat d'authentification (lorsqu'une autorité est représentée par plusieurs agents, l'identité de l'agent permet de connaître précisément la clé d'agent qui a été utilisée);

- heure de création du certificat d'authentification (cette donnée peut servir à des fins d'audit ou lorsque la durée de validité du certificat n'est pas connue; après écoulement d'un certain temps, défini par la politique de sécurité, les certificats trop anciens peuvent être rejetés);
- période de validité (pas avant, pas après) du certificat d'authentification (cette donnée peut être prise en compte si la politique de sécurité du répondeur le permet; sinon, l'heure d'expiration sera calculée à partir de l'heure de création selon les critères définis par la politique de sécurité du répondeur);
- politique de sécurité applicable au certificat d'authentification;
- numéro de référence du certificat, qui est unique parmi tous les certificats d'authentification du même agent d'autorité;
- type de certificat;
- identité ou attributs de l'entité à laquelle le certificat d'authentification est destiné (lorsque cette valeur existe, les entités peuvent la contrôler et la rejeter si elle est incorrecte. Les identités ou les attributs peuvent être, par exemple, des noms de personne, ou des identités de processus d'application ou de machine).

Les paragraphes ci-après définissent des éléments supplémentaires concernant les différents types de certificats d'authentification.

Des profils peuvent être définis dans le cadre de normes d'application afin de spécifier les éléments obligatoires et/ou les éléments facultatifs.

#### 6.1.4.1 Certificats d'authentification en ligne

Un certificat d'authentification en ligne est créé par un tiers caution par le biais d'une demande directe d'un déclarant. Il est généralement transmis au vérificateur comme partie d'informations AI pour échange.

Les certificats d'authentification en ligne peuvent contenir, par exemple, les éléments supplémentaires suivants:

- identificateur distinctif de l'entité principale;
- empreinte numérique des données pour l'authentification de l'origine des données;
- clé symétrique attribuée à l'entité principale pour l'authentification et identification de l'algorithme à utiliser conjointement avec cette clé; ces informations devront être tenues confidentielles;
- méthode d'authentification utilisée pour l'obtention du certificat d'authentification;
- méthode(s) d'authentification acceptant l'utilisation de ce certificat;
- identification de la méthode à utiliser pour protéger le certificat d'authentification lors d'un transfert et paramètres associés nécessaires à cette protection (par exemple, épreuve, numéro unique, clé de protection).

#### 6.1.4.2 Certificats d'authentification hors ligne

Un certificat d'authentification hors ligne associe une identité à une clé cryptographique. Il est créé par une autorité sans que le déclarant ni le vérificateur ait besoin d'interagir directement avec cette autorité. Ces certificats sont généralement employés pour les mécanismes d'authentification utilisant des algorithmes de chiffrement asymétrique. Ils peuvent être transmis à un vérificateur comme partie des informations AI pour échange.

Les certificats d'authentification hors ligne peuvent contenir, par exemple, les éléments supplémentaires suivants:

- identité de l'entité principale;
- clé publique attribuée à l'entité principale par l'autorité d'authentification et identification de l'algorithme à utiliser conjointement avec cette clé.

La validité de ces certificats peut être annulée par le biais d'un certificat de révocation ou d'une table de révocation.

#### 6.1.4.3 Certificats de révocation

Un certificat de révocation sert à annuler un certificat d'authentification hors ligne. Il indique à quel moment un certificat déterminé a été révoqué. Ces informations sont mises en mémoire et consultées chaque fois qu'un certificat est présenté afin de déterminer si le certificat d'authentification présenté est encore valide.

Les certificats de révocation peuvent contenir, par exemple, les éléments supplémentaires suivants:

- identité de l'entité principale, d'un groupe d'entités principales ou d'une autorité;
- heure et date de révocation du certificat d'authentification hors ligne;
- numéro de référence du certificat révoqué.

#### 6.1.4.4 Listes de certificats de révocation

Une liste de certificats de révocation est une liste certifiée de tous les certificats d'authentification ayant été révoqués, qui indique également à quel moment et à quelle date la liste a été constituée. Ces informations sont mises en mémoire et consultées chaque fois qu'un certificat est présenté afin de déterminer si le certificat d'authentification présenté est encore valide.

Une liste de certificats de révocation peut comprendre les éléments suivants:

- des certificats de révocation;
- des identificateurs renvoyant aux certificats de révocation;
- les certificats d'authentification révoqués;
- des identificateurs renvoyant aux certificats d'authentification révoqués;
- la date de constitution de la liste;
- la date de constitution de la prochaine liste.

#### 6.1.4.5 Chaînes de certificats

Les certificats d'authentification sont toujours protégés afin de fournir une authentification de l'origine des données à partir d'un tiers caution. Si le vérificateur ne dispose pas d'informations AI pour vérification afin de contrôler l'origine du certificat, une chaîne de certificats peut être utilisée. Un certificat, provenant d'une autre autorité, atteste les informations AI pour vérification utilisées pour valider l'origine du premier certificat.

Une chaîne de certificats peut être utilisée de manière récurrente, chaque certificat attestant les informations AI pour vérification utilisées pour valider l'origine du certificat précédent. La chaîne fournit ainsi un *trajet de certification* composé d'autorités depuis le vérificateur jusqu'à l'entité principale. Le vérificateur doit décider seul de la confiance qu'il peut accorder à chaque certificat de la chaîne, en se fondant sur les informations qu'il détient ou qu'il peut obtenir d'un tiers habilité.

## 6.2 Fonctionnalités

Le présent paragraphe présente un modèle général d'authentification en termes de fonctions génériques.

### 6.2.1 Informations d'état d'authentification

Ces informations représentent l'état d'authentification conservé entre deux invocations des services d'authentification. Elles peuvent comporter:

- des clés cryptographiques de session;
- des numéros séquentiels de messages.

Ces informations doivent être stockées de manière sûre. Elles sont détenues par les fournisseurs de ces services.

### 6.2.2 Services liés à la gestion

Les services liés à la gestion d'authentification peuvent comporter la distribution d'informations descriptives, de mots de passe ou de clés (par le biais de la gestion de clés), aux entités devant exécuter une authentification. Ils peuvent aussi impliquer l'utilisation d'un protocole entre les entités qui communiquent et les entités fournissant des services d'authentification. La gestion d'authentification peut aussi comporter la révocation d'informations d'authentification.

#### 6.2.2.1 Installation

Le service installation installe les informations AI pour déclaration et les informations AI pour vérification. Il peut se décomposer en plusieurs sous-services: inscription, validation et confirmation.

#### 6.2.2.1.1 Inscription

Le service inscription commande à une autorité de sécurité l'enregistrement de certaines informations d'authentification associées à une entité principale. Ces informations comprennent un identificateur distinctif qui est fourni soit par l'entité principale ou par l'autorité de sécurité. Ce service est invoqué par l'entité principale, par une autre entité ou par une autorité de sécurité. (L'autorité de sécurité chargée de l'enregistrement peut exiger de l'entité principale qu'elle donne des assurances à l'appui de la validation de son inscription.) A ce moment-là, l'entité principale est candidate à l'entrée dans un domaine de sécurité, mais elle n'a pas encore été reconnue comme membre de ce domaine. Aucun échange pour authentification n'est encore possible à ce moment précis.

#### 6.2.2.1.2 Validation

Le service validation, assuré au nom de l'autorité du domaine de sécurité, introduit une entité principale dans un domaine de sécurité.

La validation des informations AI pour vérification associées à une entité principale peut impliquer une communication entre l'autorité de sécurité et une autre entité, qui n'est pas nécessairement exécutée dans l'environnement OSI. Le service validation provoque l'affectation d'un identificateur distinctif aux informations AI pour vérification.

#### 6.2.2.1.3 Confirmation

Le service confirmation est invoqué après le service validation. Il renvoie à l'entité principale ou à d'autres entités des informations spécifiques. La forme la plus simple d'informations renvoyées est un accusé de réception ou un rejet pour l'installation. Autres formes:

- certificat d'authentification hors ligne;
- identificateur distinctif accepté;
- informations AI pour déclaration.

A la suite d'une confirmation, l'entité principale peut être authentifiée.

### 6.2.2.2 Modification d’informations AI

Ce service est utilisé, au nom d'une entité principale ou d'un gestionnaire, pour modifier des informations d'authentification.

### 6.2.2.3 Distribution

Ce service permet à une entité d'acquérir suffisamment d'informations AI pour vérification pour pouvoir contrôler des informations AI pour échange.

### 6.2.2.4 Désactivation

Ce service, qui est invoqué au nom d'une autorité de sécurité, entraîne l'établissement d'un état interdisant temporairement à une entité principale de se faire authentifier.

### 6.2.2.5 Réactivation

Ce service, qui est invoqué au nom d'une autorité de sécurité, annule l'état établi par le service désactivation.

### 6.2.2.6 Désinstallation

Ce service entraîne la suppression d'une entité principale d'un groupe d'entités principales authentifiables. Il peut être décomposé en plusieurs sous-services: invalidation, notification et annulation d'inscription.

#### 6.2.2.6.1 Invalidation

Le service invalidation est une action exécutée par un administrateur de sécurité, consistant à révoquer les informations AI pour vérification et/ou à modifier les informations de statut associées à une entité principale. Ce service interdit à une entité principale d'effectuer une authentification.

#### 6.2.2.6.2 Notification

Le service notification peut être invoqué par l'autorité de sécurité après le service invalidation. Il signale à l'entité principale son invalidation et peut également lui transmettre des informations sur les conditions de sa réinscription.

#### 6.2.2.6.3 Annulation d'inscription

Le service annulation d'inscription entraîne la suppression d'une entité principale d'un domaine de sécurité. Il correspond à la suppression de l'identité de l'entité principale et des informations AI pour vérification associées. Ce service est invoqué par une autorité de sécurité.

### 6.2.3 Services liés au fonctionnement

#### 6.2.3.1 Acquisition

Le service acquisition permet à un déclarant ou à un vérificateur d'obtenir les informations requises pour produire des informations AI pour échange spécifiques dans une instance d'authentification. Ce service peut exiger une interaction avec un tiers caution (par exemple un serveur d'authentification).

Les données d'entrée peuvent être les suivantes:

- type d'échange pour authentification;
- identificateur distinctif de l'entité principale;
- identité du vérificateur;
- type d'informations AI pour déclaration (par exemple: mot de passe, clé);
- informations AI pour déclaration (par exemple: valeur du mot de passe);
- type d'informations AI pour échange;
- validité (dates et heures de début et d'expiration).

Les données de sortie peuvent être les suivantes:

- état (succès ou échec);
- informations requises pour produire les informations AI pour échange;
- validité (dates et heures de début et d'expiration).

#### 6.2.3.2 Création

Ce service est demandé par un déclarant pour créer des informations AI pour échange et/ou pour traiter des informations AI pour échange reçues.

Les données d'entrée peuvent être les suivantes:

- type d'échange pour authentification;
- identificateur distinctif de l'entité principale;
- informations requises pour produire des informations AI pour échange en sortie de service acquisition;
- référence aux informations mémorisées concernant l'état d'authentification;
- informations AI pour échange reçues du vérificateur;
- type d'informations AI pour échange reçues;
- identité du vérificateur;
- information AI pour déclaration.

Les données de sortie peuvent être les suivantes:

- état (succès nécessité d'autres transferts, ou échec);
- référence aux informations mémorisées concernant l'état d'authentification;
- informations AI pour échange à transférer au vérificateur.

Lors de la première invocation du service création pendant un échange pour authentification, le type d'échange pour authentification peut être fourni en entrée si le déclarant est l'initiateur de l'authentification. Lors de la même invocation du service, une référence attribuée aux informations mémorisées concernant l'état d'authentification est retournée en sortie. Lors des invocations suivantes pendant le même échange, les données en entrée et en sortie ne figureront pas mais la référence aux informations mémorisées concernant l'état d'authentification pourra être fournie en entrée.

Les informations concernant l'état d'authentification sont mémorisées à l'intérieur du service pour être réutilisée à des fins d'authentification jusqu'à réception d'un état «succès» ou «échec».

Si l'état «nécessité d'autres transferts» est retourné, le déclarant devra, après réception d'informations AI pour échange d'une autre entité, avoir recours au service création. Il pourra être amené à effectuer plusieurs opérations de ce type (c'est-à-dire recourir au service création avec les précédentes informations concernant l'état d'authentification et les informations AI pour échange reçues) jusqu'à ce que l'état «succès» ou «échec» soit signalé. Le service permet ainsi d'utiliser différentes techniques y compris des échanges multilatéraux de questions/réponses, de même que les échanges requis par certains procédés à apport nul de connaissance.

#### 6.2.3.3 Vérification

Un vérificateur invoque ce service pour vérifier des informations AI pour échange reçues d'un déclarant et/ou pour créer des informations AI pour échange afin de les transférer au déclarant.

Les données en entrée peuvent être les suivantes:

- type d'échange pour authentification;
- informations requises pour produire des informations AI pour échange en sortie d'un service acquisition;
- référence aux informations mémorisées concernant l'état d'authentification;
- informations AI pour échange reçues du déclarant;
- informations AI pour vérification.

Les données en sortie peuvent être les suivantes:

- état (succès, nécessité d'autres transferts, ou échec);
- référence aux informations mémorisées concernant l'état d'authentification;
- informations AI pour échange à transférer au déclarant (en cas d'état «nécessité d'autres transferts»);
- identificateur distinctif de l'entité principale (en cas d'état «succès»);
- validité (dates et heures de début et d'expiration);
- indicateur d'authentification mutuelle.

Lors de la première invocation du service vérification pendant un échange pour authentification, le type d'échange pour authentification peut être fourni en entrée, si le vérificateur est l'initiateur de l'authentification. Lors de la même invocation du service, une référence attribuée aux informations mémorisées concernant l'état d'authentification est retournée en sortie. Lors des invocations suivantes pendant le même échange, les données en entrée et en sortie ne figureront pas mais la référence aux informations mémorisées concernant l'état d'authentification pourra être fournie en entrée.

Les informations concernant l'état d'authentification sont mémorisées à l'intérieur du service pour être réutilisées à des fins d'authentification jusqu'à réception d'un état «succès» ou «échec».

Lorsque l'état retourné est «succès», l'identificateur distinctif de l'entité principale est également renvoyé.

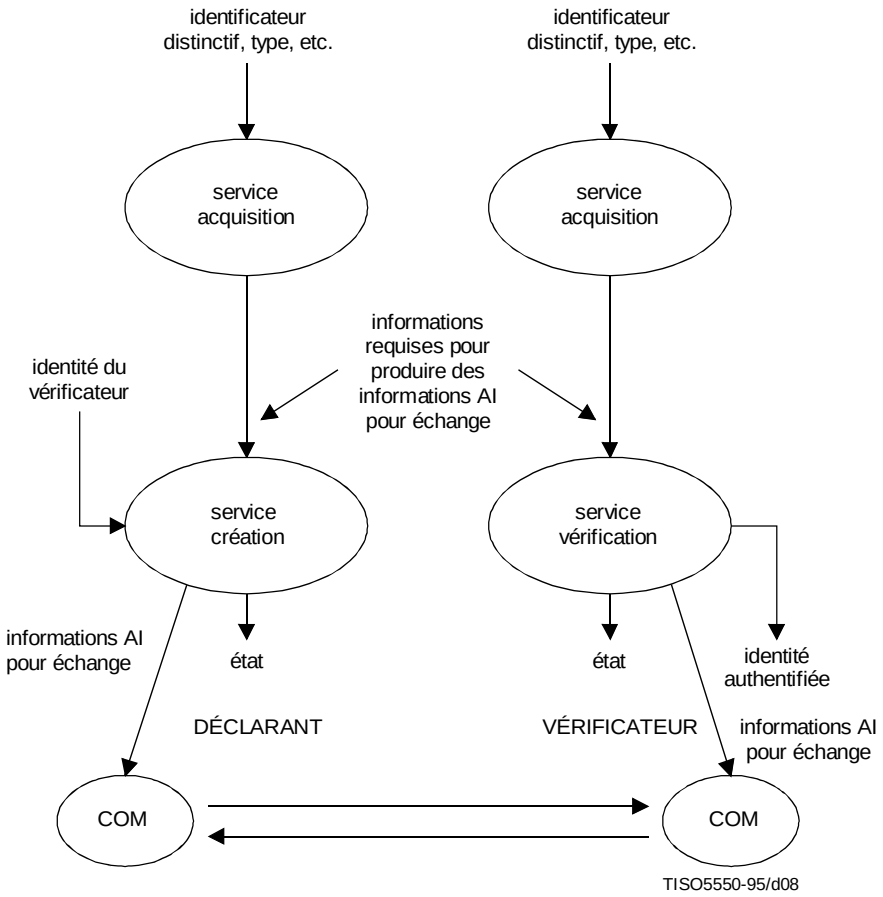
#### 6.2.3.4 Création et vérification

Dans le cas d'authentification mutuelle, ces deux services peuvent être réunis en un seul. Les données en entrée et en sortie constituent alors la réunion des données en entrée et en sortie des deux services.

NOTE – Les services création et vérification ne transfèrent aucune donnée. L'existence d'un transfert de données est liée à l'environnement dans lequel a lieu l'authentification. Ce sujet ne relève pas du domaine d'application de la présente Recommandation | Norme internationale.

#### 6.2.3.5 Exemple de flux d'informations

La Figure 8 fournit un exemple de flux d'informations liées à l'invocation des services acquisition, création et vérification, tels qu'ils sont utilisés pour fournir l'authentification (à des processus d'application par exemple).




NOTE – Dans cet exemple, le service acquisition est représenté comme étant invoqué à la fois par le déclarant et par le vérificateur. Dans la pratique, il n'est invoqué que par l'un des deux ou n'est pas invoqué du tout. Bien que le flux d'informations s'écoule entre les services création et vérification, aucun de ceux-ci n'est censé invoquer des primitives de communication.

**Figure 8 – Exemple de flux d'informations entre services opérationnels liés**

# 7 Caractéristiques des mécanismes d'authentification

Les mécanismes d'authentification faisant partie du domaine d'application de la présente Recommandation | Norme internationale peuvent se fonder sur les principes a), d) et e) définis en 5.3. Le principe d) implique le recours à un tiers caution tel qu'il est décrit en 5.5.2 mais, dans ce cas, les mécanismes dépendront en définitive des principes a) et e). Dans les systèmes ouverts, l'authentification d'entités principales distantes repose le plus souvent sur le principe a), qui fait appel à des mots de passe ou à des clés.

## 7.1 Symétrie/Asymétrie

L'authentification d'entités principales distantes repose souvent sur des secrets qui prennent la forme de mots de passe ou de clés. L'authentification implique la preuve de la connaissance du secret. Les méthodes permettant une telle démonstration sont classées en deux grandes catégories:

– *méthodes symétriques:* les deux entités partagent des informations d'authentification communes;

– *méthodes asymétriques:* les informations d'authentification ne sont pas toutes partagées par les deux entités.

Des exemples de méthodes symétriques sont les suivants:

- un mot de passe;
- une épreuve, chiffrée par une technique de clé symétrique.

Des exemples de méthodes asymétriques sont les suivants:

- les techniques de clé asymétriques;
- les techniques permettant de vérifier la possession d'informations sans qu'aucune partie de celles-ci soit révélée.

## 7.2 Utilisation de techniques cryptographiques et non cryptographiques

Les mécanismes d'authentification fondés sur la connaissance (voir 5.3) se différencient également par l'utilisation d'algorithmes cryptographiques pour la protection des informations d'authentification. Les techniques cryptographiques symétriques, asymétriques ou mixtes peuvent être employées en vue d'assurer l'intégrité et, parfois, la confidentialité de ces informations.

Les techniques non cryptographiques utilisent notamment des mots de passe et des tables de questions/réponses. Un exemple de techniques cryptographiques est l'utilisation du chiffrement pour la protection des mots de passe lors des transmissions.

## 7.3 Types d'authentification

L'authentification met en jeu deux entités. Dans l'authentification unilatérale, une entité agit comme déclarant et l'autre comme vérificateur. Dans l'authentification mutuelle, chaque entité est à la fois déclarante et vérificatrice. L'authentification mutuelle peut être assurée par le même mécanisme d'authentification dans les deux sens ou par des mécanismes différents.

### 7.3.1 Authentification unilatérale

L'authentification unilatérale peut être obtenue de trois façons:

- un seul transfert d'informations d'authentification, par exemple pour la méthode des numéros uniques;
- trois transferts d'informations d'authentification, pour la méthode des épreuves; ou
- plus de trois transferts d'informations d'authentification, pour certains mécanismes utilisant les techniques à apport nul de connaissance.

Les cas cités ci-dessus supposent que le déclarant est l'initiateur de l'authentification. Si le vérificateur est l'initiateur de l'authentification, le nombre de transferts est différent (pour plus de détails, voir 8.2).

### 7.3.2 Authentification mutuelle

L'utilisation de ce type d'authentification n'entraîne pas obligatoirement le doublement du nombre de transferts et ne requiert pas l'utilisation du même mécanisme d'authentification dans les deux sens du transfert.

Dans le cas de mécanismes d'authentification utilisant trois transferts d'informations d'authentification pour une authentification unilatérale, l'authentification mutuelle n'exige aucun transfert supplémentaire. Une demande d'épreuve peut être associée à l'envoi d'une autre épreuve utilisée par le vérificateur (agissant comme un déclarant) pour s'authentifier auprès du déclarant (qui agit alors comme vérificateur).

### 7.3.3 Accusé de réception de l'authentification

Dans certains cas, il est utile d'avoir un accusé de réception du résultat (acceptation ou refus) de l'authentification d'une entité. Cet accusé de réception peut être attesté ou se présenter simplement sous la forme d'une réponse par oui ou par non, sans aucune garantie. Cela nécessite un transfert supplémentaire.

# 8 Mécanismes d'authentification

## 8.1 Classification par vulnérabilité

Les mécanismes d'authentification peuvent eux aussi être la cible d'attaques, ce qui limite leur efficacité (voir 5.8).

Dans le présent paragraphe, les mécanismes d'authentification utilisés pour l'authentification dans la phase de transfert sont classés en fonction des risques auxquels ils résistent. Les mécanismes décrits se fondent tous sur le principe de la connaissance [voir 5.3 a)].

Ils sont tous applicables à l'authentification d'entité et certains d'entre eux peuvent également servir pour l'authentification de l'origine des données, par exemple une empreinte numérique des données dans l'échange pour authentification.

Les classes de mécanismes d'authentification suivantes sont définies:

- classe 0: sans protection;
- classe 1: protection contre la divulgation;
- classe 2: protection contre la divulgation et la réexécution sur différents vérificateurs;
- classe 3: protection contre la divulgation et la réexécution sur le même vérificateur;
- classe 4: protection contre la divulgation et la réexécution sur le même ou sur différents vérificateurs.

NOTE – Dans les classes 1 à 4, le terme «protection contre la divulgation» implique la protection des informations AI pour déclaration contre la divulgation.

D'autres classes peuvent être définies, selon les besoins. Certaines classes de protection comportent des sous-classes. Les sous-classes ne sont pas nécessairement exhaustives.

Les informations AI pour échange correspondant à chaque classe de protection sont indiquées sur les schémas.

Si l'on utilise une fonction de chiffrement dans le cadre du service création, les informations AI pour déclaration, éventuellement assorties d'autres informations, seront utilisées pour former la clé. Si une fonction de chiffrement est utilisée dans le cadre du service vérification, les informations AI pour vérification, éventuellement assorties d'autres informations reçues au cours de l'échange pour authentification, seront utilisées pour former la clé.

Les échanges pour authentification suivants sont décrits du point de vue du déclarant et sont toujours lancés par celui-ci. Pour les échanges lancés par le vérificateur, voir 8.2. Les échanges décrits sont applicables à l'authentification unilatérale. Pour les échanges applicables à l'authentification mutuelle, voir 8.4. Dans certains cas, on a besoin d'un accusé de réception du fait que l'authentification a réussi ou n'a pas réussi. Un transfert additionnel de données peut être nécessaire à cette fin mais cette opération n'est pas décrite dans cet article. Les services visés par le présent article sont définis au 6.2.

Dans les schémas qui suivent, les crochets [...] indiquent un élément facultatif des informations transférées, qui n'est inséré que dans certaines circonstances.

L'élément facultatif [empreinte digitale numérique] sera présent si l'origine des données est authentifiée et absent dans le cas contraire. On obtiendra par exemple une empreinte digitale numérique en utilisant un algorithme de chiffrement asymétrique, soit pour chiffrer simplement les données ou pour créer une valeur de contrôle cryptographique des données utilisant la clé privée du signataire. Dans le cas de l'authentification d'origine des données, le transfert des données auxquelles se rapporte l'empreinte numérique peut s'effectuer de manière totalement indépendante des moyens de communication utilisés pour les mécanismes ci-après, ou peut en partager l'utilisation.

### 8.1.1 Classe 0 (sans protection)

Dans cette classe, les informations AI pour déclaration sont simplement envoyées, en même temps que l'identificateur distinctif, en tant qu'informations AI pour échange du déclarant au vérificateur. L'exemple le plus simple est l'envoi d'un mot de passe. La classe 0 utilise un mécanisme d'authentification symétrique. Cette classe de protection est vulnérable à la divulgation d'informations d'authentification et à la réexécution.

Le service création produit les informations AI pour échange, comme le montre la Figure 9, directement à partir de ses données d'entrée.

Le service vérification contrôle que les informations AI pour déclaration reçues (par exemple un mot de passe) correspondent aux informations AI pour vérification associées à l'identificateur distinctif reçu.

Les mécanismes de la classe 0 s'appliquent à la fois à l'authentification d'entité et à l'authentification d'origine des données.

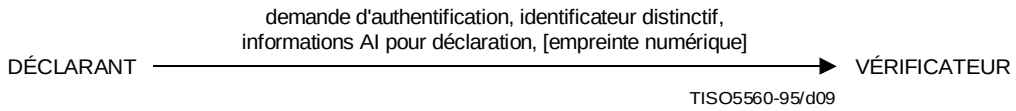



**Figure 9 – Mécanisme de classe 0 (sans protection)**

### 8.1.2 Classe 1 (protection contre la divulgation)

Cette classe fournit une protection contre la divulgation d'informations AI pour déclaration. Les mécanismes de la classe 1 s'appliquent à la fois à l'authentification d'entité et à l'authentification de l'origine des données.

Ces mécanismes appliquent une fonction de transformation aux informations AI pour déclaration, éventuellement associées à l'identificateur distinctif, qui sont ensuite transférées avec cet identificateur distinctif. Les véritables informations AI pour déclaration ne sont pas transmises par la voie de communication. On peut par exemple:

- envoyer un mot de passe transformé par une fonction univoque (telle qu'une valeur de contrôle cryptographique ou une fonction de condensation);
- envoyer une empreinte numérique chiffrée selon une clé secrète;
- envoyer un mot de passe chiffré selon une clé de confidentialité; ou
- envoyer une empreinte numérique signée au moyen d'une clé privée.

Ces mécanismes s'appliquent à la fois à l'authentification d'entité et à l'authentification de l'origine des données. Ils sont exposés aux attaques par réexécution mais offrent une protection contre la divulgation des informations AI pour déclaration. Par exemple, le mot de passe transformé peut être réexécuté au niveau de l'échange protocolaire; toutefois, le mot de passe en clair, utilisable au niveau de l'interface avec le système, n'est pas divulgué.

Le service création utilise les informations AI pour déclaration et, si nécessaire, l'identificateur distinctif et/ou une empreinte numérique, comme données d'entrée dans une opération de transformation cryptographique qui produit les informations AI pour échange (voir la Figure 10).

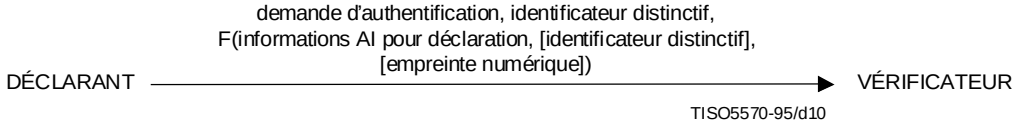



**Figure 10 – Mécanisme de classe 1 (protection contre la divulgation)**

Les fonctions de transformation (F) peuvent prendre l'une des formes suivantes, par exemple:

a) dans le cas d'une fonction univoque, la fonction de vérification répète la fonction univoque en utilisant les informations AI pour vérification à la place des informations AI pour déclaration et compare le résultat avec les informations AI pour échange reçues;

b) en cas d'utilisation d'un algorithme symétrique, la fonction de vérification utilise les informations AI pour vérification pour déchiffrer les informations AI pour échange reçues; puis elle vérifie l'exactitude du déchiffrement en s'assurant qu'il contient des caractéristiques distinctives telles que l'identificateur distinctif du déclarant, l'empreinte numérique correcte, un mot de passe ou une valeur constante;

c) dans le cas d'une signature numérique, la fonction de vérification recalcule l'empreinte numérique à partir des données reçues et utilise les informations AI de vérification pour s'assurer que la signature reçue est valide pour cette empreinte.

En outre, pour l'authentification d'origine des données, l'empreinte digitale numérique contenue dans les informations AI pour échange est comparée à une empreinte numérique régénérée des données nécessitant une authentification.

NOTE – Lorsque l'identificateur distinctif est combiné aux informations AI pour déclaration, une attaque exhaustive est rendue plus difficile. Les entités principales ne subissent pas d'attaque globale; seule une attaque sur une entité principale précise peut être menée.

Pour assurer la confidentialité, la fonction de transformation ne doit pas avoir d'inverse ou, si elle est inversable, cet inverse doit être mathématiquement inviolable par les correspondants par rapport auxquels les informations AI pour déclaration (et l'empreinte numérique) doivent être tenues confidentielles.

### 8.1.3 Classe 2 (protection contre la divulgation et la réexécution sur différents vérificateurs)

Cette classe de protection assure une protection contre la divulgation des informations AI pour déclaration et contre la réexécution sur différents vérificateurs, mais pas contre la réexécution sur le même vérificateur. Elle ressemble à la classe 1, à ceci près qu'un élément de données possédant une caractéristique propre au vérificateur visé est intégré en tant que données d'entrée de la fonction de transformation. Cela permet d'assurer une protection supplémentaire.

### 8.1.4 Classe 3 (protection contre la divulgation et la réexécution sur le même vérificateur)

Cette classe de protection assure une protection contre la divulgation des informations AI pour déclaration et contre la réexécution sur le même vérificateur.

Les mécanismes à numéro unique appartenant à cette classe comportent des fonctions de transformation combinées à des informations uniques qui assurent une protection contre la réexécution sur le même vérificateur. Les informations AI pour déclaration et le numéro unique sont transformés et transférés en même temps que l'identificateur distinctif.

Les sources de numéros uniques peuvent appartenir, par exemple, à l'un des types suivants:

a) *nombre aléatoire ou pseudo-aléatoire* – Ce nombre n'est intentionnellement pas répété pendant toute la durée de vie des informations AI pour déclaration. S'il est compris dans une fourchette suffisamment étendue, les risques (probabilités) de réutilisation du même nombre aléatoire ou pseudo-aléatoire sont réduits;

b) *horodatage* – Le numéro unique est une valeur d'horodatage obtenue auprès d'une source sécurisée qui reste unique pendant toute la durée de vie des informations AI pour déclaration; les valeurs d'horodatage trop anciennes ou déjà utilisées sont rejetées;

c) *compteur* – Le numéro unique est la valeur d'un compteur incrémenté tant que les mêmes informations AI pour déclaration sont utilisées;

d) *chaînage cryptographique* – Le numéro unique est une valeur calculée à partir du contenu des précédentes données échangées par blocs concaténés entre le déclarant et le vérificateur.

On peut s'assurer de l'unicité de ce numéro à l'extérieur du déclarant en le concaténant avec des données uniques pour le déclarant (telles que son propre identificateur distinctif).

Il est également possible d'avoir recours à une combinaison de ces techniques pour produire un numéro unique.

Les fonctions de transformation (F) peuvent être, par exemple, des trois types suivants:

a) *fonction univoque* – Le numéro unique, les informations AI pour déclaration et, sur option, l'identificateur distinctif, sont transformés par une fonction univoque. Le numéro unique est également transmis de manière que le vérificateur puisse effectuer la même transformation;

b) *algorithme asymétrique* – Lorsque les informations AI pour déclaration sont une clé privée, le numéro unique est signé d'après cette clé privée;

c) *algorithme symétrique* – Lorsque les informations AI pour déclaration sont une clé secrète, le numéro unique est chiffré d'après cette clé secrète.

Cette sous-classe s'applique à la fois à l'authentification d'entité et à l'authentification de l'origine des données.

Le service création produit un numéro unique puis effectue le chiffrement à partir des données d'entrée suivantes:

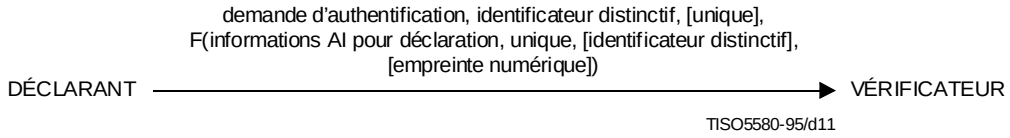
– numéro unique;

– informations AI pour déclaration;

– identificateur distinctif (facultatif);

– empreinte numérique (pour l'authentification de l'origine des données).

Il produit les informations AI pour échange comme le montre la Figure 11.




**Figue 11 – Sous-classe 3 – Mécanisme à numéro unique**

Le service vérification déchiffre et vérifie la validité des informations AI pour échange en utilisant les informations AI pour vérification. Il s'assure également que le numéro unique n'a pas déjà été reçu. Si le numéro a déjà été reçu, cela veut dire qu'une réexécution a eu lieu. En outre, pour l'authentification d'origine des données, l'empreinte numérique contenue dans les informations AI pour échange est comparée à une empreinte numérique régénérée des données reçues.

NOTE – L'utilisation du terme *chaînage cryptographique* correspond ici à la définition du *chaînage de blocs* dans l'ISO/CEI 10116.

### 8.1.5 Classe 4 (protection contre la divulgation et la réexécution sur le même vérificateur ou sur des vérificateurs différents)

#### 8.1.5.1 Sous-classe 4a – Mécanismes à numéro unique

Cette sous-classe de protection est identique à la classe 3, sauf qu'un élément de données contenant une caractéristique unique pour le vérificateur prévu est injecté dans la fonction de transformation lors de l'échange. Cela assure une protection supplémentaire.

#### 8.1.5.2 Sous-classe 4b – Mécanismes à épreuves

Les mécanismes à épreuves ont pour but de contrer les attaques par réexécution, c'est-à-dire de garantir que toute tentative d'authentification effectuée en réexécutant des informations AI pour échange échouera. En réponse à une demande d'authentification, le vérificateur émet une épreuve à l'intention du déclarant sous la forme d'un élément de données à valeur unique. Le déclarant transforme par une certaine fonction les informations de l'épreuve ainsi que les informations AI pour déclaration et retourne le résultat de la transformation au vérificateur.

Les mécanismes à épreuves impliquent donc un transfert en trois temps:

- envoi d'une demande d'authentification;
- envoi d'une épreuve;
- envoi d'une réponse contenant une valeur obtenue à partir des informations AI pour déclaration, éventuellement associée à l'identificateur distinctif, ainsi que les informations d'épreuve transformées par une fonction (F) appropriée.

Dans le cas général, l'identificateur distinctif peut être envoyé soit avec la demande d'authentification ou avec la réponse finale.

Les fonctions de transformation (F) utilisées par ce type de mécanismes peuvent être, par exemple, des trois types suivants:

a) *fonction univoque* – L'épreuve et les informations AI pour déclaration sont transformées par une fonction univoque;

b) *algorithme asymétrique* – Lorsque les informations AI pour déclaration sont une clé privée, l'épreuve est signée d'après cette clé privée;

c) *algorithme symétrique* – Lorsque les informations AI pour déclaration sont une clé secrète, l'épreuve est chiffrée d'après cette clé secrète.

Une particularité du mécanisme d'épreuves est le fait que la question posée peut dépendre de l'identité reçue dans la demande d'authentification: c'est ce qu'on appelle un mécanisme d'épreuves spécialisées. Dans ce cas, l'identificateur distinctif accompagne obligatoirement la demande d'authentification. Une quatrième fonction de transformation est encore possible:

d) *fonction non cryptographique* – Par exemple utilisation d'une table questions/réponses appariées; l'entité qui pose la question demande une réponse particulière. Autre exemple: une empreinte biométrique, comme un système à empreinte vocale.

Cette sous-classe s'applique à la fois à l'authentification d'entité et à l'authentification de l'origine des données.

Le service création produit une demande d'authentification (qui doit être, dans le cas d'une question spécialisée, être assortie d'un identificateur distinctif). A la réception de cette demande, le service vérification émet une épreuve unique en tant qu'informations AI pour échange .

Le service création crée ensuite les informations AI pour échange en transformant les données d'entrée comme le montre la Figure 12.

Dans le cas d'une fonction univoque, le service vérification répète la transformation en utilisant les informations AI pour vérification au lieu des informations AI pour déclaration; puis il les contrôle en les comparant aux informations AI pour échange reçues. Afin de répéter cette fonction, le vérificateur doit forcément disposer de l'identificateur distinctif et des données auxquelles le service s'applique. Dans le cas d'autres transformations, le service vérification répète la transformation ou calcule une fonction inverse et vérifie le contenu au moyen des informations AI pour vérification.

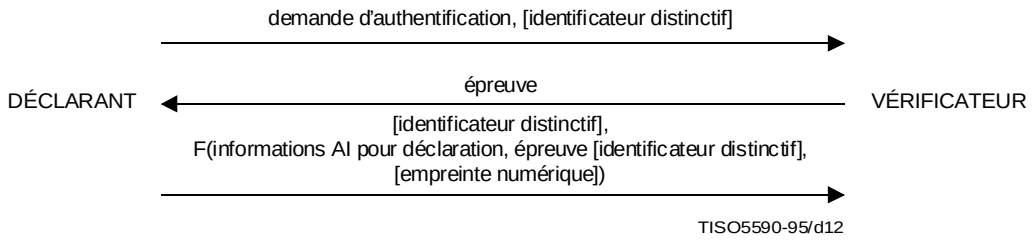



**Figure 12 – Sous-classe 4b – Mécanismes à épreuves**

### 8.1.5.3 Sous-classe 4c – Mécanismes à épreuves spécialisées et chiffrées

Ces mécanismes impliquent aussi un transfert en trois temps des informations:

- envoi d'une demande d'authentification et d'un identificateur distinctif;
- envoi d'une épreuve et d'informations AI pour vérification, éventuellement associées à l'identificateur distinctif, transformées par une fonction (F) appropriée;
- envoi de la réponse comprenant les informations de l'épreuve.

Les fonctions de transformation (F) utilisées par ce type de mécanismes peuvent être, par exemple:

a) *algorithme asymétrique* – Lorsque les informations AI pour déclaration sont une clé privée, l'épreuve est chiffrée d'après la valeur de la clé publique correspondante;

b) *algorithme symétrique* – Lorsque les informations AI pour déclaration sont une clé secrète, l'épreuve est chiffrée d'après la valeur de cette clé et cryptée par l'entité qui questionne.

Ce type de mécanisme s'applique à l'authentification d'entité mais pas à l'authentification de l'origine des données.

Le service création produit une demande d'authentification. A la réception de cette demande et de l'identificateur distinctif, le service vérification émet une question unique. Celle-ci est ensuite traitée par une fonction de transformation pour produire des informations AI pour échange comme le montre la Figure 13.

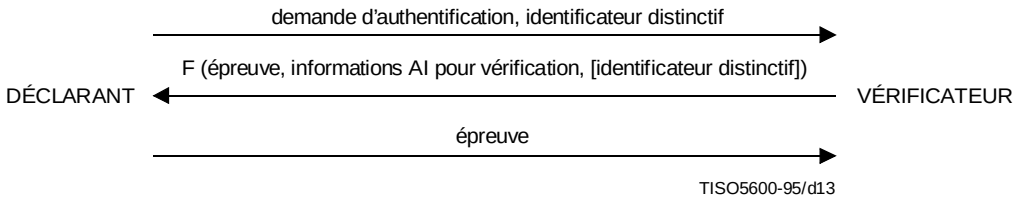



**Figure 13 – Sous-classe 4c – Mécanisme à épreuves spécialisées et chiffrées**

Le service création effectue ensuite la transformation inverse en utilisant les informations AI pour déclaration à la place des informations AI pour vérification pour obtenir l'épreuve qui est alors retournée pour servir d'informations AI pour échange. A noter que seules des transformations à chiffrement sont applicables dans ce mécanisme.

Le service vérification effectue un contrôle final en comparant la question à celle qui a été créée précédemment.

#### 8.1.5.4 Sous-classe 4d – Mécanismes à réponse calculée

Les mécanismes de cette classe impliquent également un transfert en trois temps des informations:

- envoi d'une demande d'authentification comprenant un choix de valeurs à sélectionner et des informations d'identité;
- envoi d'une épreuve indiquant les valeurs qui ont été choisies par le vérificateur;
- envoi d'une réponse comprenant un numéro unique, l'épreuve ou les valeurs choisies pour calculer la réponse, ainsi que les informations AI pour déclaration, transformées par une fonction appropriée.

Une technique à apport nul de connaissance peut, par exemple, servir à la sélection d'un ensemble de «problèmes» que le déclarant doit résoudre sans révéler exactement sa méthode.

Les échanges peuvent être répétés pour obtenir un niveau élevé de fiabilité quant à l'identité. On se protège ainsi contre des usurpations d'identité par un intrus qui pourrait calculer la réponse correcte pour certaines des valeurs (mais pas pour toutes) qu'un vérificateur pourrait choisir. Si on se limite à un seul échange, il peut se produire que le vérificateur choisisse, par hasard, une valeur pour laquelle l'intrus connaît la réponse correcte. En augmentant le nombre d'échanges, on réduit la probabilité de succès d'une telle attaque.

Le service création produit d'abord un numéro unique et un choix de valeurs, puis les met dans les informations AI pour échange, comme représenté sur la Figure 14.

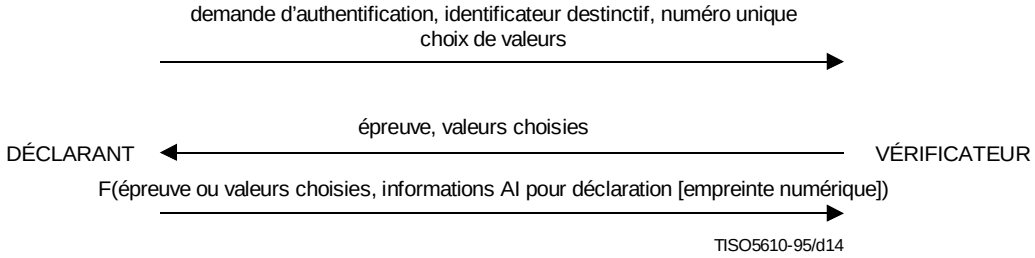



**Figure 14 – Sous-classe 4d – Mécanismes à réponse calculée**

Le service vérification choisit des valeurs parmi celles qui sont proposées, et émet une épreuve pour créer les secondes informations AI pour échange.

Le service création exécute une transformation sur l'épreuve ou sur les valeurs choisies en utilisant les informations AI pour déclaration.

Le service vérification effectue enfin la transformation inverse en utilisant des informations AI pour vérification et vérifie les valeurs reçues.

## 8.2 Lancement du transfert

En 8.1, les échanges décrits sont lancés par le déclarant par le biais d'une *demande d'authentification*. Toutefois, pour l'authentification d'entité, les mêmes sous-classes de mécanismes peuvent impliquer un échange lancé par le vérificateur à l'aide d'une *invitation à l'authentification*. Dans ce cas, le nombre de transferts sera différent. Le Tableau 1 du 8.5 indique le nombre de transferts nécessaires dans chaque cas.

## 8.3 Utilisation de certificats d'authentification

On peut classer les mécanismes d'authentification en fonction des moyens utilisés pour acquérir les informations AI pour vérification. Ces moyens seront par exemple:

- certificats d'authentification en ligne;
- certificats d'authentification hors ligne;
- informations AI pour vérification fournies d'avance, par exemple au moyen de voies sécurisées.

Un certificat d'authentification peut être utilisé afin de donner une preuve d'authenticité conformément au principe décrit en 5.3 d). Le certificat d'authentification prouve qu'un tiers caution a associé un identificateur distinctif à des informations AI pour vérification spécifiques.

## 8.4 Authentification mutuelle

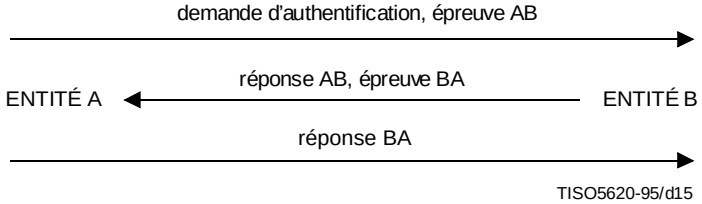
Pour les sous-classes de mécanismes impliquant un seul transfert (sous-classes 1, 2, 3 et 4a), un échange de forme identique peut être utilisé dans chaque sens pour l'authentification mutuelle.

Pour la sous-classe 4b, le même type de mécanisme peut être utilisé dans les deux sens. La première épreuve peut accompagner la demande d'authentification et la transformée de cette épreuve peut être jointe à la deuxième épreuve (voir la Figure 15). Cela exige le même nombre de transferts que dans le cas d'une authentification unilatérale.

De même, pour la sous-classe 4c, la transformée de la première épreuve peut accompagner la demande d'authentification, et la transformée de la seconde épreuve être envoyée avec la première épreuve.

La sous-classe 4b peut être utilisée en combinaison avec un mécanisme de type 4c. Les deux épreuves sont intégrées aux données transformées. Dans le cas d'algorithme de chiffrement symétrique, les informations AI pour déclaration et les informations AI pour vérification sont les mêmes et la transformation est effectuée une seule fois. Dans le cas d'algorithme de chiffrement asymétrique, les deux transformations sont exécutées à chaque extrémité.

Dans la sous-classe 4d, il faut au moins trois transferts pour effectuer une authentification unilatérale, alors que l'authentification mutuelle en nécessite au moins quatre.




ENTITÉ A initiateur d'authentification
ENTITÉ B répondeur d'authentification

NOTE – Pour connaître le détail des réponses et des transferts d'identificateurs distinctifs, voir la description des sous-classes et les figures correspondantes.

**Figure 15 – Authentification mutuelle utilisant des mécanismes à épreuves**

## 8.5 Résumé des classes de caractéristiques

Le Tableau 1 résume les vulnérabilités et les caractéristiques des différentes classes et sous-classes. Les caractéristiques y figurant sont celles que décrit l'article 7.

**Tableau 1 – Vulnérabilités et caractéristiques des mécanismes**

| Sous-classes | 0 | 1 | 2 | 3 | 4a | 4b | 4c | 4d |
|---|---|---|---|---|---|---|---|---|
| *Vulnérabilités* | | | | | | | | |
| Divulgation | Oui | Non | Non | Non | Non | Non | Non | Non |
| Réexécution sur différents vérificateurs | Oui | Oui | Non | Oui | Non | Non | Non | Non |
| Réexécution sur le même vérificateur | Oui | Oui | Oui | Non | Non | Non | Non | Non |
| Attaque par relais lancée par intrus | Non | Non | Non | Non | Non | Non | Non | Non |
| Attaque par relais avec réponse d'intrus | Oui | Non | Non | Non | Non | Non | Non | Non |
| *Caractéristiques* | | | | | | | | |
| Symétrie (S)/Asymétrie (A) | S | S/A | S/A | S/A | S/A | S/A | S/A | A |
| Cryptographique (O)/ Non cryptographique (N) | N | N/O | N/O | N/O | N/O | N/O | O | O |
| Nombre de transferts | | | | | | | | |
| – initiateur déclarant | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 |
| – initiateur vérificateur | 2 | 2 | 2 | 2 | 2 | 2 | 4 | 4 |
| Authentification de l'origine des données | Oui | Oui | Oui | Oui | Oui | Oui | Non | Oui |

## 8.6 Classification par configuration

Lorsque des entités veulent s'authentifier, elles peuvent avoir besoin de recourir à un ou à plusieurs tiers caution. La relation de confiance entre chaque entité et un tiers caution quelconque doit être définie. Le modèle le plus simple ne comporte qu'un seul tiers caution; d'autres font appel à un ensemble de tiers caution en relation de confiance. Mais la configuration la plus courante comporte un ensemble de tiers caution sans relations de confiance entre eux.

### 8.6.1 Principes de modélisation n'impliquant que des tiers caution

Dans certains cas, le vérificateur ne peut avoir la garantie de l'identité de l'entité principale que s'il reçoit l'assurance de cette identité par l'intermédiaire de plusieurs tiers caution.

Lorsque trois tiers caution ou plus sont impliqués, il est nécessaire de se prémunir contre la corruption d'un ou de plusieurs tiers caution. Dans certaines politiques de sécurité, une règle de décision majoritaire peut s'appliquer.

Le présent paragraphe ne traite que le cas le plus simple, où un seul tiers caution est impliqué.

Les relations entre le déclarant, le vérificateur et une tierce partie unique peuvent être modélisées en termes de:

- phases identifiées en 5.4 (en particulier, phases de distribution, d'acquisition, de transfert et de vérification);
- connaissance d'informations initiales.

#### 8.6.1.1 Modélisation en termes de phases

Les phases sont associées aux différentes entités de la façon suivante:

- la phase de distribution s'applique entre le déclarant, le vérificateur et le tiers caution;
- la phase d'acquisition s'applique entre le déclarant et le tiers caution ou entre le vérificateur et cette tierce partie;
- la phase de transfert s'applique entre n'importe quelle paire comprenant un déclarant, un vérificateur et un tiers caution;
- la phase de vérification s'applique entre le vérificateur et le tiers caution.

Les phases d'acquisition, de transfert et de vérification peuvent utiliser un mécanisme d'authentification faisant partie des classes identifiées en 8.1.

La phase de distribution peut s'effectuer en ligne ou hors ligne. Dans ce dernier cas, elle précédera l'échange pour authentification. Il n'y a alors aucune assurance que les informations AI pour déclaration soient encore valides, c'est-à-dire qu'elles n'aient pas été révoquées.

Plusieurs procédés d'authentification peuvent être identifiés, comme le montre la Figure 16. Dans cette figure, l'entité A correspond au déclarant, et l'entité B au vérificateur. Cette figure n'est donnée qu'à titre d'illustration; elle n'est pas nécessairement exhaustive.

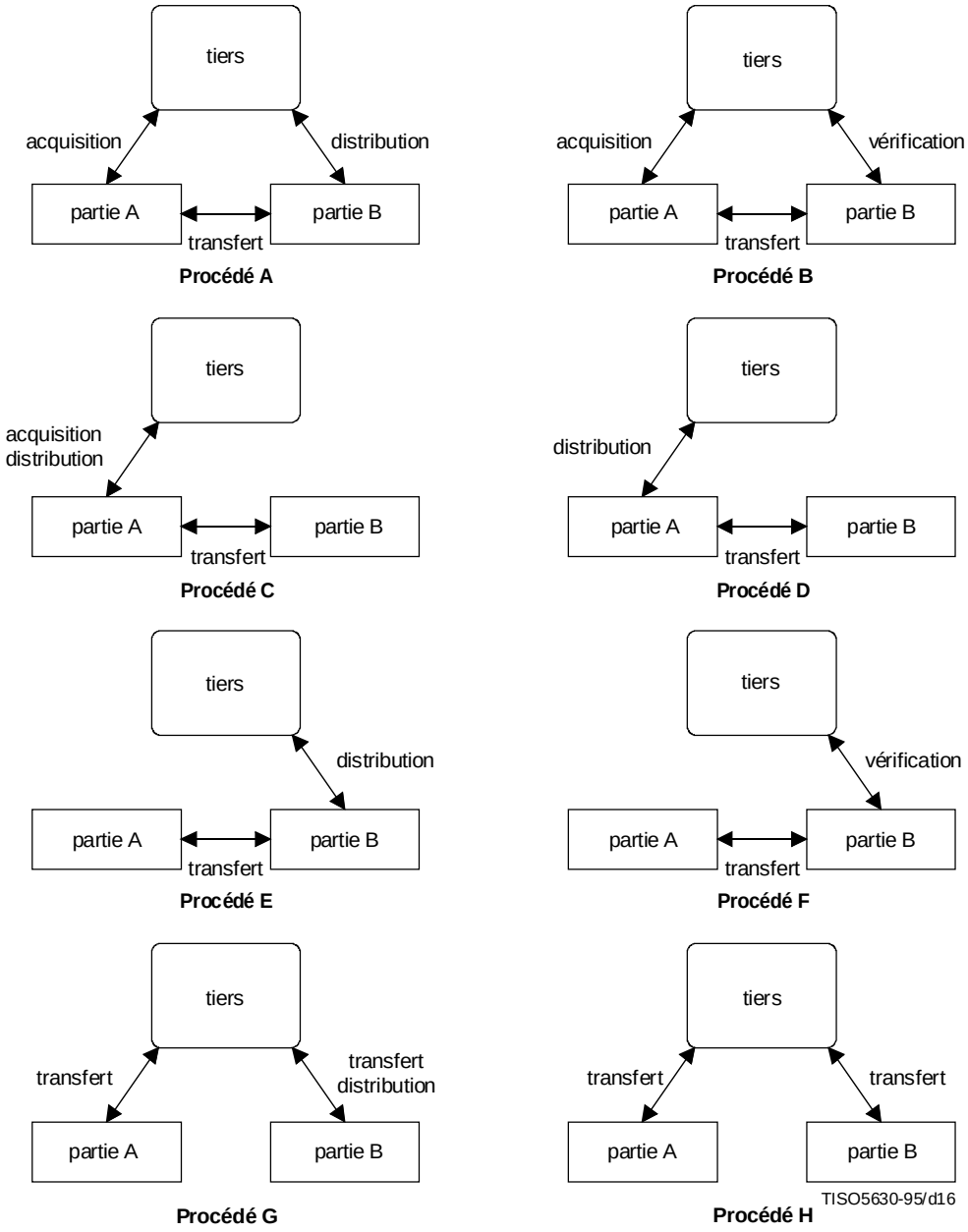



**Figure 16 – Procédés d'authentification**

Dans le procédé A, l'entité A obtient ses informations AI pour déclaration du tiers caution après un échange pour authentification avec celui-ci, et l'entité B reçoit les informations AI pour vérification de la tierce partie. L'entité B exécute la vérification au niveau local.

Dans le procédé B, l'entité A obtient ses informations AI pour déclaration du tiers caution après un échange pour authentification avec celui-ci, et l'entité B présente les informations AI pour échange reçues de l'entité A au tiers caution pour que celui-ci les vérifie.

Dans le procédé C, l'entité A obtient ses informations AI pour déclaration du tiers caution, après un échange pour authentification avec celui-ci, ainsi que les informations AI pour vérification nécessaires pour que l'entité B exécute la vérification au niveau local.

Dans le procédé D, l'entité A obtient les informations AI pour vérification, nécessaires pour que l'entité B exécute la vérification au niveau local et elle produit localement les informations AI pour échange. Les informations AI pour échange et les informations AI pour vérification sont présentées ensemble à l'entité B.

Dans le procédé E, l'entité A produit localement ses informations AI pour échange et les présente à l'entité B. Puis l'entité B obtient du tiers caution les informations AI pour vérification nécessaires pour réaliser la vérification locale.

Dans le procédé F, l'entité A produit localement ses informations AI pour échange et les présente à l'entité B. Puis l'entité B présente les informations AI pour échange reçues de l'entité A au tiers caution pour vérification.

Dans le procédé G, qui représente une relation de confiance en coupure de ligne, l'entité A produit localement ses informations AI pour échange et les présente au tiers caution qui envoie ensuite à l'entité B un certificat d'authentification accompagné des informations AI pour vérification nécessaires pour la vérification locale.

Dans le procédé H, qui représente un autre cas de relation de confiance en coupure de ligne, l'entité A produit localement ses informations AI pour échange et les présente au tiers caution qui envoie ensuite à l'entité B la notification de vérification de l'identité de l'entité A.

#### 8.6.1.2 Modélisation en termes de connaissance d'informations initiales

Avant qu'un échange pour authentification ait lieu, le déclarant (entité A) et le vérificateur (entité B) doivent disposer de certaines informations initiales. Si un tiers caution est impliqué, le déclarant ne connaît pas directement la clé publique ou la clé secrète utilisable par le vérificateur. Il existe divers types de connaissances initiales, décrites ci-après.

##### 8.6.1.2.1 Informations initiales partagées entre le déclarant et le tiers caution

Les différents cas sont les suivants:

a) clé secrète partagée entre le déclarant et le tiers caution, connue de l'un et de l'autre (techniques à clé secrète);

b) clé privée du déclarant, connue uniquement de lui (entité A); clé publique du déclarant connue du tiers caution (techniques asymétriques);

c) clé privée du déclarant connue de celui-ci et du tiers caution (techniques à apport nul de connaissance).

##### 8.6.1.2.2 Informations initiales partagées par le vérificateur et le tiers caution

Les différents cas sont les suivants:

a) clé secrète partagée entre le vérificateur (entité B) et le tiers caution, connue de l'un et de l'autre (techniques à clé secrète);

b) clé publique du tiers caution connue du vérificateur (entité B) (techniques à apport nul de connaissance et à chiffrement asymétrique).

### 8.6.2 Relations entre tiers caution participant à une authentification

#### 8.6.2.1 Tiers caution connectés

Ces tiers peuvent être indispensables à la réalisation d'un échange pour authentification. S'ils appartiennent à un même domaine de sécurité, ils peuvent détenir les informations AI pour déclaration et/ou les informations AI pour vérification des entités qui ont déjà été enregistrées dans ce domaine.

Des protocoles et/ou des procédures sont nécessaires pour garantir que différentes entités principales ne sont pas enregistrées sous le même nom dans un domaine de sécurité donné.

La disponibilité des tiers caution connectés est essentielle; sinon, les échanges d'authentification utilisant des entités tierces connectées seraient menacés de déni de service. La copie des informations d'authentification dans différentes entités tierces peut minimiser ce problème. De plus, des protocoles sont indispensables pour effectuer cette copie.

Lorsqu'il faut échanger des informations AI pour vérification ou des informations AI pour déclaration, il est nécessaire d'avoir un service d'intégrité et, dans certains cas, un service de confidentialité, entre les tiers caution à l'authentification.

Il pourra également être utile d'envisager l'échange des enregistrements d'audit tenus par les divers tiers caution à authentification en ligne du domaine de sécurité. Des protocoles sont nécessaires pour l'envoi et la réception de ces enregistrements.

#### 8.6.2.2 Tiers caution hors ligne

Les tiers caution hors ligne sont souvent appelés autorités de certification car ils peuvent délivrer des certificats d'authentification hors ligne. Aucune protection particulière n'est nécessaire pour ces derniers car ils sont protégés intrinsèquement. La disponibilité de ces certificats est essentielle; sinon, les échanges pour authentification qui les utilisent seraient menacés de déni de service. La copie de ces informations dans plusieurs répertoires de données (l'Annuaire, par exemple) peut minimiser ce problème.

# 9 Interactions avec d'autres services et mécanismes de sécurité

## 9.1 Contrôle d'accès

Avant d'être autorisés à obtenir des informations de contrôle d'accès, permettant l'accès à des ressources soumises à une politique de contrôle d'accès, il est possible que les utilisateurs aient à se faire authentifier. Le service d'authentification fournira donc les résultats de l'authentification au service de contrôle d'accès.

La révocation d'informations d'authentification peut entraîner celle de l'accès existant.

## 9.2 Intégrité des données

L'authentification peut être associée à un service d'intégrité des données pour assurer la continuité de l'authentification et pour confirmer la source des données.

Certains mécanismes d'authentification peuvent servir à distribuer, implicitement ou explicitement, un élément clé utilisable pour un service d'intégrité. Lorsque cet élément est défini implicitement, la méthode permettant de déduire cette valeur à partir des données transférées doit être connue ou spécifiée lors de l'échange pour authentification. Lorsque cet élément est défini explicitement, des données supplémentaires doivent être transférées dans l'un ou l'autre sens lors de l'échange pour authentification.

## 9.3 Confidentialité des données

Certains mécanismes d'authentification peuvent servir à distribuer, implicitement ou explicitement, un élément clé utilisable par un service de confidentialité. Lorsque cet élément est défini implicitement, la méthode permettant de déduire cette valeur à partir des données transférées doit être connue ou spécifiée lors de l'échange pour authentification. Lorsque cet élément est défini explicitement, des données supplémentaires doivent être transférées dans l'un ou l'autre sens lors de l'échange pour authentification.

## 9.4 Non-répudiation

Certains mécanismes d'authentification peuvent servir à distribuer, implicitement ou explicitement, un élément clé utilisable pour un service de non-répudiation. Lorsque cet élément est défini implicitement, la méthode permettant de déduire cette valeur à partir des données transférées doit être connue ou spécifiée lors de l'échange pour authentification. Lorsque cet élément est défini explicitement, des données supplémentaires doivent être transférées dans l'un ou l'autre sens lors de l'échange pour authentification.

## 9.5 Audit

Les informations relatives à l'authentification utilisables lors d'audits, peuvent être des types suivants:

a) résultats d'authentification (par exemple identification garantie);

b) informations liées à la révocation d'informations d'authentification;

c) informations sur la garantie de la continuité de l'authentification;

d) autres informations relatives au processus d'authentification.

# Annexe A

# Authentification d'usagers

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

## A.1 Considérations générales

Lorsque des systèmes ouverts prennent en charge l'action de personnes, l'authentification correcte des usagers peut être essentielle pour la sécurité. Le dialogue entre humains et ordinateurs peut accroître la possibilité d'intrusion par usurpation d'identité. Les méthodes d'authentification d'usagers doivent être acceptables pour les usagers tout en restant économiques et fiables. Les méthodes gênantes encouragent parfois les usagers à trouver le moyen de les contourner, ce qui augmente les risques.

L'authentification d'un usager repose sur au moins l'un des principes d'authentification suivants:

a) la connaissance de quelque chose;

b) la possession de quelque chose;

c) une caractéristique propre à l'usager;

d) l'acceptation du fait qu'un tiers caution identifié a établi l'identité de l'usager;

e) le contexte (par exemple l'adresse d'origine de la demande).

Un processus d'authentification d'usager suppose généralement la mise en concordance de justificatifs d'identité présentés par l'usager avec des informations d'authentification fournies lors de la phase d'installation.

### A.1.1 Authentification par la connaissance

L'information d'authentification la plus couramment utilisée dans ce cas est un mot de passe. L'usager accédant à un système présente un mot de passe que le système authentificateur compare avec la valeur correspondante dans une liste de mots de passe afin de confirmer l'identité de l'usager. Les mots de passe devraient être difficiles à deviner et être gérés avec soin. Si ce n'est pas le cas, ils risquent d'être involontairement divulgués.

### A.1.2 Authentification par la possession

Dans ce cas, on utilise un jeton physique tel que:

a) cartes magnétiques; ou

b) cartes à circuit(s) intégré(s).

Si l'usager présente une carte magnétique lors de l'accès au système, le système authentificateur lit les informations d'authentification de ce jeton physique et les compare à celles qui sont stockées afin de confirmer l'identité de l'usager.

Les cartes magnétiques sont vulnérables dans la mesure où elles sont facilement imitables et peuvent être détenues par une autre personne que leur possesseur, dont l'authentification ne sera plus possible.

Si l'usager présente une carte à circuit(s) intégré(s) lors de l'accès au système, le système authentificateur lit les informations d'authentification de ce jeton physique et crée les informations AI pour échange afin de confirmer l'identité de l'usager. L'un des avantages de ces cartes est qu'elles sont difficilement imitables.

Deux cas de figure peuvent être envisagés:

– lorsque la carte à circuit(s) intégré(s) peut authentifier le titulaire, il y a alors un double procédé d'authentification, où l'usager est authentifié par le vérificateur; cela revient, par transitivité, à authentifier directement l'usager;

– lorsque la carte à circuit(s) intégré(s) ne peut pas authentifier le titulaire et si elle est détenue par une autre personne, l'authentification de l'usager échoue.

### A.1.3 Générateur de mots de passe liés au temps

L'un des types de mécanismes d'authentification d'usagers consiste en un dispositif portatif fonctionnant comme un générateur de mots de passe temporaires. Les informations AI pour échange sont alors une combinaison des éléments suivants:

– informations secrètes stockées à l'intérieur du dispositif;

– date et heure;

– numéro personnel d'identification (PIN) introduit directement par l'usager sur un clavier d'entrée de numéro PIN intégré à l'appareil.

Les informations AI pour échange s'affichent ensuite sur le dispositif. Elles sont envoyées par l'usager (en texte clair) au système vérificateur. Il est possible que celui-ci doive se synchroniser avec la carte. Ce type de mécanisme exige que la personne qui cherche à se faire authentifier:

a) possède le dispositif adéquat;

b) connaisse le numéro PIN.

### A.1.4 Authentification par les caractéristiques propres à l'usager

Les mots de passe sont susceptibles d'être divulgués s'ils ne sont pas gérés avec soin; les jetons physiques risquent d'être volés ou imités, dans le cas des cartes magnétiques. Il existe une classe de méthodes d'authentification d'usagers ne présentant pas ces défauts, qui se fondent sur certaines caractéristiques immuables des individus, telles que:

– la signature manuscrite;

– l'empreinte digitale;

– l'empreinte vocale;

– l'empreinte rétinienne;

– des caractéristiques de clavier dynamiques.

Il existe deux importantes classes de systèmes de signatures manuscrites: statiques et dynamiques. Ces dernières peuvent comporter des éléments relatifs à la pression, au temps et à la direction.

L'analyse des caractéristiques de clavier dynamiques constitue un processus d'authentification continue.

Dans la phase d'inscription, un usager enregistre son identité sur le système d'inscription. L'usager exécute la procédure requise, par exemple en écrivant sa signature ou en appuyant un doigt sur un clavier, ou encore en prononçant certains mots. La procédure est répétée jusqu'à obtention d'informations de référence fiables. Le système analyse la valeur caractéristique de l'action de l'usager et l'enregistre comme étant le profil de celui-ci.

Au cours des phases de transfert et de vérification, l'usager présente son identité et réexécute la procédure requise. Le système de vérification compare l'empreinte obtenue au profil enregistré.

## A.2 Processus agissant au nom d’un usager

Dans certaines circonstances, un usager peut souhaiter agir sans être présent. Il aura alors, à l'intérieur du système, une représentation dont la durée de vie peut être indépendante de la présence effective de l'usager.

La représentation agissant au nom de l'usager, les actions de celui-ci peuvent se poursuivre sans qu'il soit directement impliqué. L'usager peut, par exemple, se connecter et utiliser ensuite d'autres ordinateurs sans se connecter.

Les représentations peuvent aussi être associées à des mécanismes supplémentaires qui établissent un lien entre la durée de vie des représentations et la présence effective de l'usager.

# Annexe B

# Authentification dans le modèle OSI

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

La relation des services de sécurité avec le modèle de référence de base OSI est définie dans ISO 7498-2. La présente annexe résume les éléments ayant trait à l'authentification.

Deux services de sécurité sont examinés:

- l'authentification de l'entité homologue;
- l'authentification de l'origine des données.

## B.1 Authentification de l'entité homologue

Ce service peut être utilisé lors de l'établissement de la phase de transfert de données d'une connexion (ou au cours de ce transfert) afin de confirmer l'identité d'une ou de plusieurs entités connectées à une ou plusieurs autres entités. Il est disponible dans les protocoles en mode connexion ou sans connexion. L'authentification de l'entité homologue est possible de manière unilatérale ou mutuelle.

## B.2 Authentification de l'origine des données

Ce service confirme la source d'une unité de données. Il n'assure aucune protection contre la duplication ou la modification des unités de données.

## B.3 Utilisation de l'authentification dans les couches OSI

L'authentification de l'entité homologue ou de l'origine des données ne concerne que les couches OSI suivantes:

- couche Réseau (couche 3);
- couche Transport (couche 4);
- couche Application (couche 7).

### B.3.1 Utilisation de l'authentification dans la couche Réseau

Dans la couche Réseau, l'authentification de l'entité homologue permet de confirmer l'identité des entités de réseau. Ce service authentifie les nœuds de réseau, les nœuds de sous-réseau ou les relais.

L'authentification de l'origine des données permet de confirmer l'identité de la source d'une unité de données. Cette source peut être un nœud de réseau, un nœud de sous-réseau ou un relais.

Les mécanismes utilisés par la couche Réseau sont intégrés à cette couche.

### B.3.2 Utilisation de l'authentification dans la couche Transport

Dans la couche Transport, l'authentification de l'entité homologue permet de confirmer l'identité des entités de transport. Ce service authentifie les systèmes d'extrémité. Il n'est pas possible d'authentifier des applications différentes prises en charge par les mêmes systèmes d'extrémité.

L'authentification de l'origine des données permet de confirmer l'identité de la source d'une entité de données. Cette source est un système d'extrémité.

Les mécanismes utilisés par la couche Transport sont intégrés à cette couche.

### B.3.3 Utilisation de l'authentification dans la couche Application

Dans la couche Application, l'authentification de l'entité homologue permet de confirmer l'identité des entités d'application prises en charge par les systèmes d'extrémité. Ce service authentifie les entités d'application ou les processus d'application. Il est possible d'authentifier des entités d'application ou des processus d'application différents pris en charge par les mêmes systèmes d'extrémité.

L'authentification de l'origine des données permet de confirmer l'identité de la source d'une unité de données. Cette source peut être une entité ou un processus d'application.

Les mécanismes utilisés dans la couche Application peuvent être dans la couche Application ou dans la couche Présentation. Si elle est invoquée au niveau de la couche Application, l'authentification peut aussi utiliser des services d'authentification fournis par la couche Réseau ou la couche Transport.

# Annexe C

## Utilisation de numéros uniques ou d'épreuves pour lutter contre la réexécution

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

### C.1 Numéros uniques

Les numéros uniques sont produits par le déclarant. Le même numéro unique ne doit jamais être accepté deux fois par le même vérificateur. Pour éviter que cela se produise, il existe divers moyens. Certaines techniques qui semblent en théorie valables ne sont pas applicables dans la réalité. Ainsi, s'il fallait garder trace de tous les numéros uniques déjà reçus et utilisés au cours d'un échange pour authentification, le volume de mémoire occupée augmenterait proportionnellement au nombre d'authentifications réussies. Pour des raisons de coûts et de performances, cette technique peut se révéler inacceptable.

Un moyen de réduire le volume de mémoire nécessaire du côté du vérificateur consiste à garder une trace de tous les numéros uniques acceptés pendant seulement une période de temps. Ceci conduit à introduire un élément d'horodatage dans le numéro unique de sorte que seuls les numéros «récents» soient mémorisés par le vérificateur. Dans la pratique, une fenêtre de temps de quelques minutes peut suffire pour, à la fois, limiter l'occupation de mémoire et minimiser les problèmes de synchronisation entre les deux références temporelles utilisées par l'entité principale et par le vérificateur.

Pour éviter les dénis de service, il est préférable d'empêcher les collisions involontaires de numéros uniques produits par des entités principales différentes. Pour cela, le numéro unique devrait être choisi dans une fourchette suffisamment large. Cette fourchette dépend du nombre maximal d'authentifications qui doivent être effectuées dans un laps de temps donné (par exemple en une seconde) du côté d'un même vérificateur. Lorsque le temps de référence utilisé par l'entité principale ne permet pas d'obtenir un nombre suffisamment grand, un numéro unique aléatoire peut être ajouté à l'horodatage pour élargir la fourchette de variation du numéro unique.

### C.2 Epreuves

Les épreuves sont produites par le vérificateur. La même épreuve ne doit jamais être proposée deux fois par le même vérificateur. Il existe plusieurs façons d'éviter que cela se produise.

Certaines techniques qui semblent en théorie valables ne sont pas applicables dans la réalité. Ainsi, s'il fallait garder trace de toutes les épreuves déjà proposées, le volume de mémoire occupée augmenterait proportionnellement au nombre d'authentifications réussies en utilisant ces épreuves. Pour des raisons de coûts et de performances, cette technique peut se révéler inacceptable.

Les différents moyens de réduire le volume de mémoire nécessaire du côté du vérificateur sont les suivants:

- associer une valeur séquentielle à chaque épreuve et ne conserver que la dernière valeur séquentielle émise;
- associer un chiffre aléatoire à chaque épreuve; afin de réduire à une valeur acceptable la probabilité que la même épreuve soit proposée deux fois, le chiffre doit être choisi à l'intérieur d'une fourchette suffisamment étendue, bien que ce procédé enfreigne la règle voulant que la même épreuve ne soit jamais utilisée deux fois;
- associer une valeur d'horodatage à chaque épreuve;
- associer une valeur d'horodatage à un chiffre aléatoire.

# Annexe D

# Protection contre certaines formes de piratage sur l'authentification

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

## D.1 Piratage par écoute et réexécution

Il existe deux manières de réexécuter un échange d'informations AI:

- sur le même vérificateur;
- sur un vérificateur différent.

Cette dernière façon de réexécuter est possible dès que les informations AI pour vérification d'une entité principale sont connues de plusieurs vérificateurs. Lorsque la réexécution réussit, c'est un cas particulier de l'usurpation d'identité.

Ces deux cas de réexécution peuvent être contrés au moyen d'épreuves. Celles-ci sont créées par le vérificateur. La même épreuve ne doit jamais être proposée deux fois par le même vérificateur, ce qui peut être réalisé de plusieurs manières (voir l'Annexe C).

## D.2 Réexécution sur le même vérificateur

Ce type de piratage peut être contré par l'utilisation de numéros uniques ou d'épreuves.

Les numéros uniques sont créés par le déclarant. Le même numéro unique ne doit jamais être accepté deux fois par le même vérificateur. L'Annexe C explique les différents moyens d'utiliser cette méthode.

## D.3 Réexécution sur un vérificateur différent

Ce type de piratage peut être contré au moyen d'épreuves. En variant, on peut y parer en utilisant, lors du calcul des informations AI pour échange, toute caractéristique spécifique du vérificateur, telle que son nom, son adresse de couche réseau ou, plus généralement, tout attribut propre aux vérificateurs partageant les mêmes informations AI pour vérification.

## D.4 Piratage par interception et relais

### D.4.1 Piratage direct

Ce type de piratage implique que l'intrus soit l'initiateur d'authentification. Ce piratage n'est possible que si le déclarant et le vérificateur peuvent lancer tous les deux l'authentification. Ils échangent alors des informations d'authentification par l'intermédiaire d'un intrus sans se rendre compte de la présence de ce dernier, c'est-à-dire que l'intrus se fait passer pour un vérificateur auprès du déclarant et pour ce déclarant auprès du vérificateur.

Par exemple, supposons que l'intrus C se fasse passer pour le déclarant A auprès du vérificateur B. C lance une interaction avec A et avec B. C affirme à A qu'il est B et demande à A de s'authentifier auprès de B. Il dit aussi à B qu'il est A et qu'il veut s'authentifier.

Lors du processus d'authentification, A agit comme déclarant auprès de B (en réalité auprès de C qui se fait passer pour B) et fournit donc à C l'information nécessaire pour qu'il se fasse authentifier par B. B agit comme le vérificateur et fournit également à C l'information qui lui est nécessaire pour jouer le rôle du vérificateur. Une fois l'authentification effectuée, B considérera C comme A qu'il vient d'authentifier.

Pour contrer ce type de piratage, il est nécessaire de recourir à une méthode de protection contre la réexécution sur un autre vérificateur:

a) l'entité qui lance l'interaction est toujours le déclarant; ou

b) les informations AI pour échange fournies par le déclarant diffèrent selon qu'il est l'initiateur ou le répondeur d'une demande d'authentification ou le répondeur à une invitation d'authentification. Cette différence permet au vérificateur de détecter l'interception (voir l'Annexe D pour plus de précisions).

### D.4.2 Attaques opportunistes

Ce type de piratage consiste, pour l'intrus, à s'immiscer au milieu d'un échange d'authentification, à intercepter les informations d'authentification et à les transmettre en prenant la place du déclarant.

La parade générale contre ce type de piratage nécessite l'emploi d'un service complémentaire (d'intégrité ou de confidentialité). Les informations AI pour échange sont combinées avec d'autres informations permettant au déclarant et au vérificateur, à condition qu'ils soient les interlocuteurs légitimes, de calculer une clé. La clé calculée pourra ensuite être utilisée pour ouvrir un mécanisme d'intégrité ou de confidentialité à base cryptographique.

Une autre parade est possible lorsque le réseau de communication n'est pas soumis à des interceptions internes, c'est-à-dire qu'il remet toujours à l'adresse correcte des données intactes. Dans cette situation, on peut contrer le piratage en intégrant dans l'échange les adresses de couche réseau. De cette façon, les informations AI pour échange dépendront de l'adresse de réseau.

## D.5 Forme limitée de protection contre les attaques d'intrus

Le deuxième type de piratage décrit en D.4 peut se produire lorsque l'on utilise des épreuves ou des numéros uniques. La parade consiste, pour le déclarant, à employer un indicateur précisant si la réponse suit une invitation à authentification ou une demande d'authentification. Cet indicateur peut signaler soit (lorsqu'il est mis à un) que la réponse fait suite à une invitation à authentification ou (lorsqu'il est mis à zéro) que la réponse fait suite à une demande d'authentification. Lorsque l'indicateur fait partie du calcul de la réponse, il en découle que la valeur de réponse donnée par le déclarant dépendra de la valeur de l'indicateur. L'indicateur sera désigné ci-après par le terme indicateur d'invitation/demande.

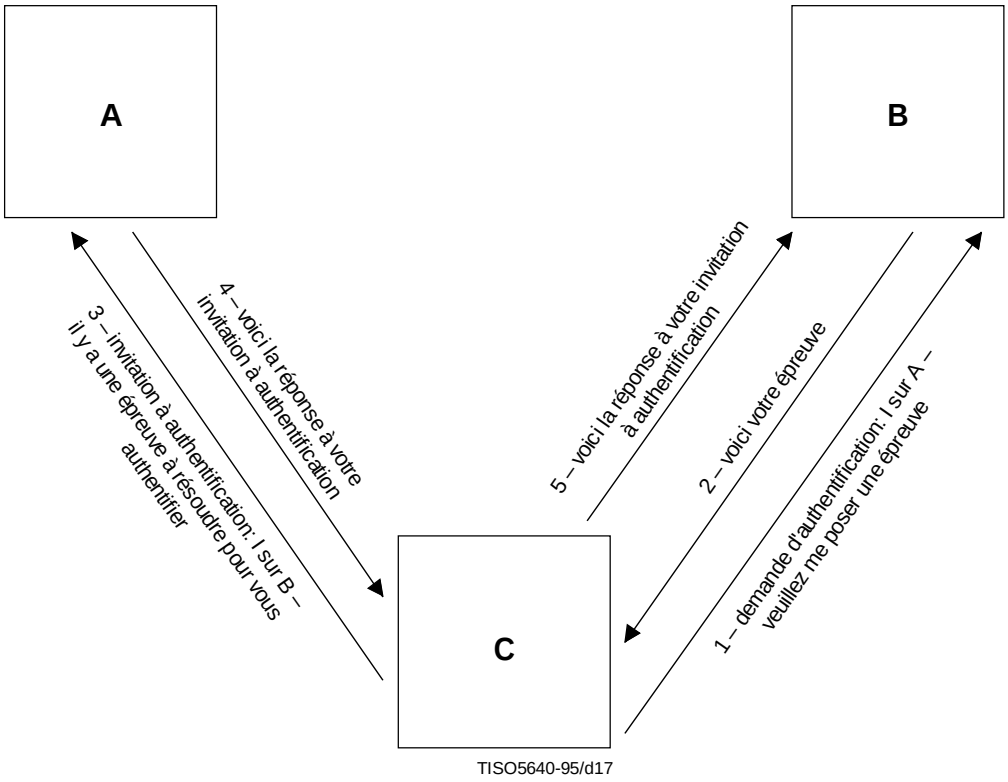
## D.6 Protocoles utilisant des épreuves proposées par le déclarant

Lorsque des épreuves sont utilisées, C se fait passer pour A et envoie une demande d'authentification à B (premier transfert). B envoie une épreuve à C (deuxième transfert). C envoie à A une invitation à authentification et transmet également l'épreuve proposée par B (troisième transfert). A calcule sa réponse à partir de l'épreuve reçue de C et de l'indicateur d'invitation/demande, qui se trouve à l'état «invitation». C transmet à B la réponse qu'il a reçue de A. B vérifie cette réponse. Puisqu'il a, à l'origine, reçu de la part de C une demande d'authentification, il attend en retour un indicateur d'invitation/demande mis à «demande». Comme il reçoit une réponse calculée avec un indicateur d'invitation/demande mis à «invitation», il rejette l'authentification (voir la Figure D.1).

Si B prend en charge à la fois les demandes d'authentification et les invitations, il doit veiller à une autre condition: lorsqu'il émet une invitation, il doit mémoriser à quel déclarant il l'a envoyée pour que C ne puisse pas l'utiliser pour un autre déclarant lorsqu'il envoie sa propre invitation (troisième transfert).

## D.7 Protocoles utilisant des numéros uniques

Lorsque des numéros uniques sont utilisés, C se fait passer pour B et émet une invitation à authentification en direction de A (premier transfert). A calcule sa réponse à partir d'un numéro unique et de l'indicateur d'invitation/demande, qui se trouve à l'état «invitation» (deuxième transfert). C transmet à B la réponse qu'il a reçue de A (troisième transfert). B vérifie cette réponse. Comme elle contient un indicateur d'invitation/demande mis à «invitation» et que B n'a pas émis d'invitation, B rejette l'authentification (voir la Figure D.2).




NOTE – Les piratages directs restent, comme expliqué en D.4.1, vulnérables aux attaques opportunistes, même si ils sont contrés au moyen de la méthode a) ou b).

**Figure D.1 – Protection contre l'intrusion en utilisant des épeuves**

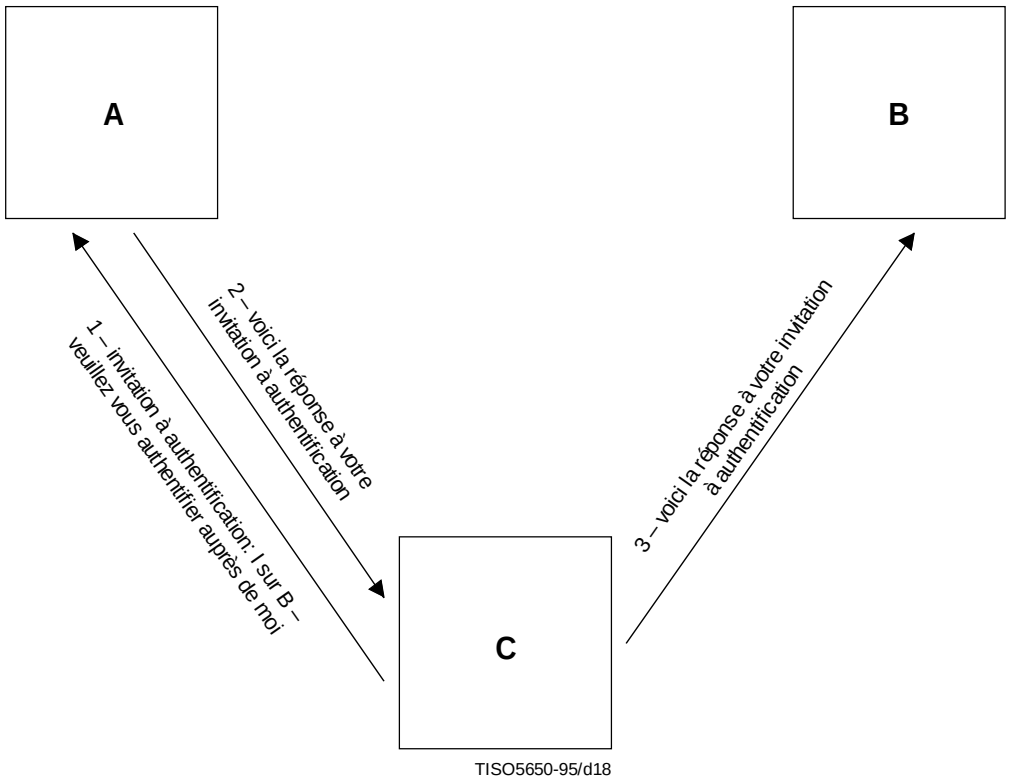



**Figure D.2 – Protection contre l'intrusion en utilisant des numéros uniques**

# Annexe E

## Bibliographie

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

ISO/CEI 9798-1:1991, *Technologies de l'information – Techniques de sécurité – Mécanismes d'authentification d'entité – Partie 1: Modèle général.*

ISO/CEI 9798-2:1994, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques.*

ISO/CEI 9798-3:1993, *Technologies de l'information – Techniques de sécurité – Mécanismes d'authentification d'entité – Partie 3: Authentification d'entité utilisant un algorithme à clé publique.*

ISO/CEI 9798-4:1995, *Technologies de l'information – Techniques de sécurité – Mécanismes d'authentification d'entité – Partie 4: Mécanismes utilisant une fonction cryptographique de vérification.*

Recommandation UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre d'authentification.*

# Annexe F

## Exemples particuliers de mécanismes d'authentification

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

Cette annexe donne deux exemples particuliers d'utilisation de mécanismes d'authentification.

### F.1 Exemple particulier de mécanisme à numéro unique avec certificat d'authentification en ligne

Cet exemple illustre l'emploi d'un mécanisme à numéro unique tel que décrit dans la classe 3 du 8.1, avec des certificats d'authentification en ligne comportant l'identificateur distinctif, une méthode de protection, un paramètre de protection et une période de validité. Dans le cas proposé en exemple, il suffit d'un seul transfert et un certificat d'authentification donné peut être utilisé plusieurs fois.

La méthode de protection indique la relation entre le paramètre de protection contenu dans le certificat et le paramètre de commande externe à utiliser pour protéger le certificat d'authentification contre un usage non autorisé. Le paramètre de commande externe peut être associé au paramètre de protection au moyen d'une relation univoque comme suit:

- le paramètre de commande externe est une valeur de validation et le paramètre de protection est le résultat de l'application d'une fonction univoque à la valeur de validation;
- le paramètre de commande externe est une clé privée et le paramètre de protection est la clé publique correspondante.

Lorsqu'une valeur de validation est utilisée comme paramètre de commande externe, elle est envoyée au vérificateur comme preuve de propriété du certificat d'authentification. Pendant son transit, la confidentialité de la valeur de validation doit toujours être garantie; elle sera par exemple envoyée sous forme chiffrée par le déclarant au vérificateur, au moyen d'une clé de confidentialité externe associée à la voie de communication ou à l'extrémité réceptrice de cette voie.

La protection de propriété et de réexécution est assurée au moyen d'un numéro unique et d'une fonction de transformation. Trois fonctions de transformation différentes (F) peuvent être utilisées selon la nature du paramètre de contrôle externe:

a) *fonction univoque* – Le numéro unique et la valeur de validation sont transformés par une fonction univoque. Le numéro unique est transmis de manière que le vérificateur puisse accomplir la même transformation;

b) *algorithme asymétrique* – Lorsque le paramètre de commande externe est une clé privée, le numéro unique est signé d'après cette clé privée;

c) *algorithme symétrique* – Lorsque le paramètre de commande externe est une clé secrète, le numéro unique est chiffré ou scellé d'après la valeur de validation utilisée comme clé secrète.

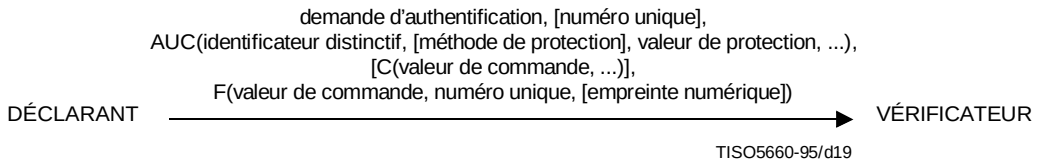
Cet exemple s'applique à la fois à l'authentification de l'origine des données et à l'authentification de l'identité. Pour l'authentification de l'origine des données, les données ou une empreinte numérique des données peuvent également être transformées par la fonction F.

Le service acquisition sert à obtenir le certificat d'authentification en ligne et un paramètre de commande externe. Le service création produit ensuite un numéro unique et effectue une transformation en utilisant les données d'entrée suivantes:

- numéro unique;
- paramètre de commande externe;
- identificateur distinctif (facultatif);
- empreinte numérique (pour l'authentification de l'origine des données).

De plus, lorsque le paramètre de commande externe est une clé de validation ou une clé de contrôle secrète, le service création envoie cette clé chiffrée de sorte que seul le vérificateur visé puisse la déchiffrer et produit les informations AI pour échange comme le montre la Figure 14.

Le service vérification contrôle la validité des informations AI pour échange en utilisant la valeur de protection contenue dans le certificat d'authentification. De plus, lorsqu'une clé de validation ou une clé de contrôle secrète est utilisée, ce service déchiffre la clé de validation ou la clé de contrôle secrète chiffrée puis vérifie qu'elle correspond à la valeur de protection. Il s'assure également que le numéro unique n'a pas déjà été reçu.




NOTES

1 AUC(...) désigne un certificat d'authentification connectée comprenant les paramètres indiqués.

2 C(...) désigne l'application d'un service de confidentialité. Cela n'est valable que si le paramètre de commande externe est une valeur de validation.

**Figure F.1 – Mécanisme à numéro unique avec certificat d'authentification en ligne**

## F.2 Mécanisme à épreuves avec certificat d'authentification en ligne

Ce mécanisme utilise un certificat d'authentification afin de fournir une preuve d'authentification utilisant le principe décrit en 5.3 d) et le mécanisme d'épreuves décrit au 8.1.5.2. Le certificat d'authentification donne la preuve qu'un tiers caution a authentifié son mandataire au moyen d'un identificateur distinctif spécifique. Ce mécanisme permet de prouver qu'un certificat d'authentification est détenu par le déclarant pour un identificateur distinctif donné.

Dans cet exemple utilisant les certificats d'authentification en ligne, ces derniers contiennent l'identificateur distinctif, une méthode de protection, un paramètre de protection et une période de validité. Cet exemple permet la réutilisation des certificats d'authentification.

La méthode de protection indique la relation entre le paramètre de protection contenu dans le certificat et le paramètre de commande externe à utiliser pour protéger le certificat d'authentification contre une utilisation non autorisée. Le paramètre de commande externe peut être associé au paramètre de protection au moyen d'une relation univoque comme la suivante:

– le paramètre de commande externe est une valeur de validation et le paramètre de protection est le résultat d'une fonction univoque appliquée à la valeur de validation;

– le paramètre de commande externe est une clé privée et le paramètre de protection est la clé publique correspondante.

Lorsqu'une valeur de validation est utilisée comme paramètre de commande externe, elle est transmise au vérificateur comme preuve de la détention du certificat d'authentification. Lors du transfert, la clé doit être protégée contre sa divulgation; elle est envoyée, par exemple, sous forme chiffrée au vérificateur, par le déclarant. Celui-ci utilisera à cette fin une clé de confidentialité externe associée à la voie de communication ou à l'extrémité réceptrice de cette voie.

La protection de propriété et de réexécution est assurée par une épreuve et une fonction de transformation. Trois fonctions de transformation différentes (F) peuvent être utilisées selon la nature du paramètre de contrôle externe:

a) *fonction univoque* – La question et la valeur de validation sont transformées par une fonction univoque;

b) *algorithme asymétrique* – Lorsque le paramètre de commande externe est une clé privée, la question est signée d'après cette clé privée;

c) *algorithme symétrique* – Lorsque le paramètre de commande externe est une clé secrète, la question est chiffrée ou scellée d'après la valeur de validation utilisée comme clé secrète.

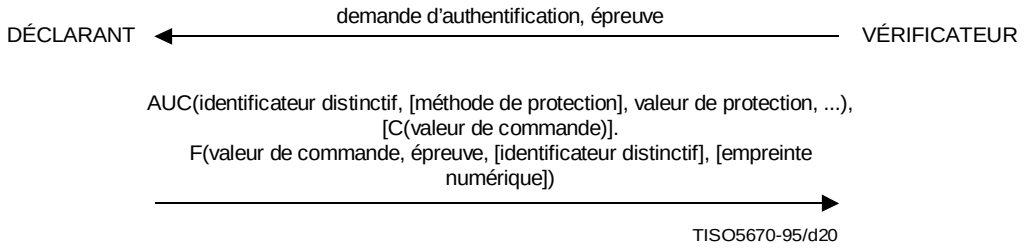
Cet exemple s'applique tant à l'authentification d'entité qu'à l'authentification d'origine des données. Pour authentifier l'origine des données, il est également possible de transformer par la fonction F les données ou une empreinte numérique de celles-ci.

Le service acquisition est utilisé pour obtenir le certificat d'authentification en ligne et un paramètre de commande externe. Le service création produit une demande d'authentification. A la réception de cette demande, le service vérification émet une épreuve à titre d'informations AI pour échange. Le service création effectue ensuite une transformation en utilisant les données d'entrée suivantes:

- épreuve;
- paramètre de commande externe;
- identificateur distinctif (facultatif);
- empreinte numérique (en cas d'authentification de l'origine des données).

De plus, lorsque la valeur de commande est une clé de validation ou une clé de commande secrète, le service création envoie cette clé chiffrée, de sorte que seul le vérificateur visé puisse la déchiffrer. Ce service produit également les informations AI pour échange comme le montre la Figure 16.

Le service vérification contrôle les informations AI pour échange en utilisant le paramètre de protection contenu dans le certificat d'authentification. De plus, lorsqu'une clé de validation ou une clé de contrôle secrète est utilisée, ce service déchiffre la valeur de validation ou la clé de contrôle secrète chiffrée et vérifie qu'elle correspond à la valeur de protection. Il s'assure également que la question correspond à celle qui avait été envoyée.




NOTES

1 AUC(...) désigne un certificat d'authentification en ligne comprenant les paramètres indiqués.

2 C(...) désigne l'application d'un service de confidentialité. Cela n'est valable que si le paramètre de commande externe est une valeur de validation.

**Figure F.2 – Mécanisme à épreuves avec certificat d'authentification en ligne**

# Annexe G

## Synoptique des fonctions d'authentification

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

<table>
<tr><td colspan="2" rowspan="3">Synoptique des fonctions de sécurité</td><td rowspan="2">Elément</td><td>Entité: déclarant, vérificateur, tiers caution, entité principale, gestionnaire</td></tr>
<tr><td>Objet informationnel: informations d'authentification</td></tr>
<tr><td colspan="2">But de l'entité: donner l'assurance de l'identité revendiquée par une entité</td></tr>
<tr><td rowspan="6">ACTIVITÉ</td><td>Entité</td><td colspan="2">Autorité de sécurité, entité principale, gestionnaire</td></tr>
<tr><td>Fonction</td><td colspan="2"></td></tr>
<tr><td>Activité de gestion associée</td><td colspan="2">– installation<br>– modification des informations AI<br>– distribution<br>– réactivation<br>– désinstallation</td></tr>
<tr><td>Entité</td><td colspan="2">– déclarant<br>– vérificateur<br>– tiers caution</td></tr>
<tr><td>Fonction</td><td colspan="2"></td></tr>
<tr><td>Activité d'exploitation associée</td><td colspan="2">– acquisition<br>– production<br>– vérification<br>– production<br>– vérification</td></tr>
<tr><td rowspan="3">INFORMATIONS</td><td>Eléments de données d'entrée/sortie gérés par l'autorité du domaine de sécurité</td><td colspan="2">Informations descriptives, par exemple: mot de passe, clé, utilisation d'un protocole, table d'épreuves/réponses, accusé de réception ou rejet, certificat en ligne, informations d'état, informations AI</td></tr>
<tr><td>Types d'informations utilisées pour l'opération</td><td colspan="2">Informations AI pour déclaration<br>Informations AI pour échange<br>Informations AI pour vérification</td></tr>
<tr><td>Informations de contrôle</td><td colspan="2">Validité<br>Informations d'état d'authentification</td></tr>
</table>