UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.813

(10/96)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE X: RÉSEAUX POUR DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

Sécurité

Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité dans les systèmes ouverts: non-répudiation

Recommandation UIT-T X.813

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX POUR DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS POUR DONNÉES	X.1–X.199
Services et fonctionnalités	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	X.200–X.299
Modèle et notation	X.200–X.209
Définitions 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
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
Réseautage	X.600–X.629
Efficacité	X.630–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
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion	X.730–X.799
SÉCURITÉ	**X.800–X.849**
APPLICATIONS OSI	X.850–X.899
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT OUVERT RÉPARTI	X.900–X.999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

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.813 de l'UIT-T a été approuvé le 5 octobre 1996. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-4.

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.

TABLE DES MATIÈRES

Résumé

La présente Recommandation | Norme internationale définit un cadre général pour la fourniture d'un service de non-répudiation. Le service de non-répudiation a pour objet de collecter, de conserver, de diffuser et de valider des preuves irréfutables concernant l'identification des expéditeurs et des destinataires participant à des transferts de données.

Introduction

Le service de non-répudiation a pour objet de collecter, de conserver, de diffuser et de valider des preuves irréfutables concernant un événement ou une action revendiqué afin de résoudre des litiges concernant la réalité ou la non-réalité de cet événement ou de cette action. Le service de non-répudiation peut être appliqué dans un certain nombre de contextes et de situations différents. Ce service peut s'appliquer à la production de données, à la conservation de données ou à la transmission de données. La non-répudiation implique la production de preuves qui peuvent être utilisées pour prouver qu'un certain type d'événement ou d'action a eu lieu, de manière que cet événement ou cette action ne puisse être répudié ultérieurement.

Dans un environnement d'interconnexion OSI (voir la Rec. X.800 du CCITT et l'ISO 7498-2), le service de non-répudiation a deux formes:

- non-répudiation avec preuve d'origine, qui est utilisée pour contrer un faux déni d'envoi des données ou de leur contenu par leur expéditeur;
- non-répudiation avec preuve de remise, qui est utilisée pour contrer un faux déni de réception des données ou de leur contenu (c'est-à-dire ce que les données représentent) par leur destinataire.

Les applications qui font usage des protocoles OSI peuvent nécessiter d'autres formes du service de non-répudiation qui soient spécifiques de classes d'application particulières. Par exemple, la messagerie MHS (Rec. UIT-T X.402 | ISO 10021-2) définit la non-répudiation du service de soumission, tandis que le système de messagerie EDI (voir la Recommandation X.435) définit la non-répudiation des services de consultation et des services de transfert.

Les concepts contenus dans le présent cadre ne sont pas limités aux communications OSI mais peuvent être interprétés plus largement afin d'inclure des usages tels que la création et la conservation des données pour usage ultérieur.

La présente Recommandation | Norme internationale définit un cadre général pour la fourniture d'un service de non-répudiation.

Ce cadre:

- développe les concepts des services de non-répudiation qui sont décrits dans la Rec. X.800 du CCITT et l'ISO 7498-2; il décrit la façon dont ces concepts peuvent être appliqués aux systèmes ouverts;
- décrit les variantes de fourniture de ces services;
- explique la relation de ces services avec d'autres services de sécurité.

Les services de non-répudiation peuvent nécessiter:

- des arbitres qui régleront les litiges qui peuvent apparaître à la suite d'événements ou d'actions répudiés;
- des tiers de confiance qui garantiront l'authenticité et l'intégrité des données à utiliser pour la vérification des preuves.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITÉ DANS LES SYSTÈMES OUVERTS: NON-RÉPUDIATION

1 Domaine d'application

La présente Recommandation | Norme internationale traite de l'application des services de sécurité dans un environnement de systèmes ouverts, où le terme «systèmes ouverts» est considéré comme visant des domaines tels que les bases de données, les applications réparties, le traitement réparti ouvert et l'interconnexion OSI. Les cadres de sécurité concernent la définition des moyens d'assurer la protection des systèmes et des objets contenus dans ces systèmes. Ils concernent également les interactions entre ces systèmes. Les cadres de sécurité ne concernent pas la méthode de construction des systèmes ou des mécanismes.

Les cadres de sécurité traitent aussi bien des éléments de données et des séquences d'opérations (mais non des éléments de protocoles) qui sont utilisés pour obtenir des services de sécurité spécifiques. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes ainsi qu'aux données échangées entre systèmes et aux données gérées par les systèmes.

La présente Recommandation | Norme internationale:

- définit les concepts fondamentaux de la non-répudiation;
- définit les services généraux de non-répudiation;
- identifie les mécanismes permettant de fournir les services de non-répudiation;
- identifie les prescriptions générales de gestion pour services et mécanismes de non-répudiation.

Comme avec d'autres services de sécurité, la non-répudiation ne peut être fournie que dans le cadre d'une politique de sécurité définie pour une application particulière. Les définitions des politiques de sécurité sont hors du domaine d'application de la présente Recommandation | Norme internationale.

Le domaine d'application de la présente Recommandation | Norme internationale ne comprend pas la spécification des détails relatifs aux échanges protocolaires qui doivent être effectués afin d'utiliser le service de non-répudiation.

La présente Recommandation | Norme internationale ne décrit pas en détail les mécanismes particuliers que l'on peut utiliser pour prendre en charge le service de non-répudiation; elle ne donne pas non plus de détails concernant les services et protocoles de gestion de sécurité qui sont utilisés à l'appui du service de non-répudiation.

Certaines des procédures décrites dans le présent cadre réalisent la sécurité en appliquant des techniques cryptographiques. Ce cadre ne dépend pas de l'utilisation d'un algorithme cryptographique ou non cryptographique particulier, ni de techniques cryptographiques particulières (c'est-à-dire symétriques ou asymétriques) bien que certaines classes de mécanismes de non-répudiation puissent dépendre de propriétés algorithmiques particulières. En fait, il est probable qu'en pratique un certain nombre d'algorithmes différents seront utilisés. Deux entités souhaitant utiliser des données protégées par cryptographie doivent toujours prendre en charge le même algorithme cryptographique.

[NOTE – Bien que l'ISO ne normalise pas les algorithmes cryptographiques, cette organisation normalise, dans l'ISO/CEI 9979, les procédures utilisées pour les enregistrer.]

Un certain nombre de types de norme différents peuvent utiliser ce cadre, à savoir:

1) les normes qui intègrent le concept de non-répudiation;
2) les normes qui spécifient des services abstraits comportant la non-répudiation;
3) les normes qui spécifient les utilisateurs d'un service de non-répudiation;
4) les normes qui spécifient les moyens de fournir le service de non-répudiation dans une architecture de système ouvert;
5) les normes qui spécifient des mécanismes de non-répudiation.

De telles normes peuvent utiliser ce cadre comme suit:

- les normes de type 1), 2), 3), 4) ou 5) peuvent utiliser la terminologie de ce cadre;
- les normes de type 2), 3), 4) ou 5) peuvent utiliser les fonctionnalités définies dans l'article 7 de ce cadre;
- les normes de type 5) peuvent être fondées sur les classes de mécanisme définies dans l'article 8 de ce cadre.

2 Références normatives

Les Recommandations et les 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. Toutes Recommandations et Normes 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 UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base*.
- Recommandation UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre d'authentification*.
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – 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 de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

3 Définitions

3.1 Définitions relatives au modèle de référence de base

La présente Recommandation | Norme internationale est fondée sur les concepts développés dans la Rec. UIT-T X.200 | ISO/CEI 7498-1 et fait usage du terme suivant, qui y est défini:

entité (N).

3.2 Définitions relatives à l'architecture de sécurité

La présente Recommandation | Norme internationale est fondée sur les concepts développés dans la Rec. X.800 du CCITT et l'ISO 7498-2 et fait usage des termes suivants, qui y sont définis:

- contrôle d'accès;
- audit (de sécurité);
- authentification;
- voie;
- valeur de contrôle cryptographique;
- cryptographie;
- intégrité (des données);
- authentification de l'origine des données;
- déchiffrement;

- signature (numérique);
- chiffrement;
- clé;
- gestion de clés;
- notarisation;
- répudiation;
- journal d'audit de sécurité; journal d'audit; journal;
- menace.

3.3 Définitions relatives à l'aperçu général des cadres de sécurité

La présente Recommandation | Norme internationale est fondée sur les concepts développés dans la Rec. UIT-T X.810 | ISO/CEI 10181-1 et fait usage des termes suivants, qui y sont définis:

- autorité de certification;
- empreinte numérique;
- fonction d'adressage dispersé;
- fonction à sens unique;
- clé privée;
- clé publique;
- certificat de liste de révocation;
- cachet;
- cacheté;
- clé secrète;
- certificat de sécurité;
- domaine de sécurité;
- jeton de sécurité;
- tiers de confiance.

3.4 Définitions supplémentaires

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

3.4.1 **preuve compromise**: preuve, qui avait été satisfaisante à un moment donné, mais en laquelle le tiers de confiance ou l'arbitre n'a plus confiance.

3.4.2 **contresignature**: signature numérique ajoutée à une unité de données déjà signée par une entité différente (par exemple un tiers habilité).

3.4.3 **preuve**: information qui, par elle-même ou par association avec d'autres informations, peut être utilisée pour résoudre un litige.

3.4.4 **générateur de preuve**: entité qui produit une preuve de non-répudiation.

NOTE – Cette entité peut être le demandeur du service de non-répudiation, l'expéditeur, le destinataire ou des parties multiples travaillant de concert (par exemple un signataire et un cosignataire).

3.4.5 **sujet de preuve**: entité dont l'implication dans un événement ou une action est démontrée par une preuve.

3.4.6 **utilisateur de preuve**: entité qui utilise une preuve de non-répudiation.

3.4.7 **vérificateur de preuve**: entité qui vérifie une preuve de non-répudiation.

3.4.8 **code d'authentification de message**: valeur de contrôle cryptographique utilisée pour assurer l'intégrité des données et l'authentification de leur origine.

3.4.9 demandeur du service de non-répudiation: entité qui demande qu'une preuve de non-répudiation soit produite pour un événement particulier ou pour une action particulière.

3.4.10 notaire: tiers de confiance chez qui les données sont enregistrées afin de pouvoir garantir plus tard l'exactitude des caractéristiques de ces données.

3.4.11 expéditeur: dans le contexte du transfert de données, entité qui expédie les données par une action qui est sujette à un service de non-répudiation.

3.4.12 destinataire: dans le contexte du transfert de données, entité qui reçoit les données par une action qui est sujette à un service de non-répudiation.

NOTE – Dans le modèle logique de non-répudiation, d'autres entités peuvent intervenir. Par exemple, le propriétaire est l'entité qui formule un message original et un agent de transfert est l'entité qui transfère le message; dans ce contexte, les entités seront assimilées à des entités expéditrices ou destinataires.

4 Abréviations

CA Autorité de certification (*certification authority*)

MAC Code d'authentification de message (*message authentication code*)

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

TTP Tiers de confiance (*trusted third party*)

5 Considérations générales sur la non-répudiation

5.1 Concepts de base de la non-répudiation

Le service de non-répudiation implique la production, la vérification et l'enregistrement de preuves, ainsi que la consultation et la revérification ultérieures de ces preuves, en cas de besoin. Les litiges ne peuvent être résolus que si les preuves ont été enregistrées au préalable.

L'objet du service de non-répudiation décrit dans ce cadre est de fournir une preuve au sujet d'un événement particulier ou d'une action particulière. Le service de non-répudiation peut être demandé par des entités autres que celles qui participent à l'événement ou à l'action. Exemples d'action pouvant être protégée par un service de non-répudiation:

- expédition d'un message X.400;
- insertion d'un article dans une base de données;
- invocation d'une opération distante.

Lorsqu'il s'agit de messages, l'identité de l'expéditeur et l'intégrité des données doivent être confirmées pour prouver l'origine des messages. Pour apporter la preuve d'une remise des données, il faut confirmer l'identité du destinataire et l'intégrité des données remises. Dans certains cas, des preuves peuvent également être requises concernant le contexte (par exemple, la date, l'heure, l'emplacement de l'expéditeur/destinataire).

Ce service offre les options supplémentaires suivantes, qui peuvent être utilisées en cas de tentative de répudiation:

- production de preuve;
- enregistrement de preuve;
- vérification de la preuve produite;
- consultation et revérification de la preuve.

Les litiges peuvent être réglés directement entre parties prenantes, par examen des preuves. Un litige peut parfois devoir être réglé par un arbitre, qui évalue les preuves et détermine si l'action ou l'événement litigieux a eu lieu. L'arbitrage ne peut être assuré efficacement que si les parties au litige acceptent l'autorité de l'arbitre. Pour que les preuves fournies soient acceptées par l'arbitre, il faut généralement qu'elles soient confirmées par un ou par plusieurs tiers de confiance. En option, l'arbitre peut être le tiers de confiance qui confirme la preuve. Les mécanismes de non-répudiation font appel à un certain nombre de types de tiers de confiance et de formes de preuve.

5.2 Rôles d'un tiers de confiance

Un ou plusieurs tiers de confiance peuvent être impliqués dans le service de non-répudiation.

Les tiers de confiance qui assurent la non-répudiation sans être activement impliqués dans chaque utilisation du service sont appelés «*tiers de confiance déconnectés*». Un tiers de confiance qui est activement impliqué dans la production ou dans la vérification de preuves est appelé «*tiers de confiance connecté*». Un tiers de confiance connecté qui fait office d'intermédiaire dans toutes les interactions est appelé «*tiers de confiance en ligne*».

Un tiers de confiance peut être appelé à enregistrer et/ou à recueillir des preuves; il peut également être appelé à attester la validité des preuves. Un certain nombre de tiers de confiance peuvent être impliqués dans divers rôles (par exemple les rôles de notaire, de pointeur temporel, de surveillant, de certificateur de clé, de producteur de signature, de vérificateur de signature et d'autorité de remise). Un même tiers de confiance peut agir au titre d'un ou de plusieurs de ces rôles.

Dans le rôle de producteur de preuve, un tiers de confiance coopère avec un demandeur de service de non-répudiation pour produire des preuves.

Dans le rôle d'enregistreur de preuve, un tiers de confiance enregistre des preuves qui pourront être consultées ultérieurement par un utilisateur de preuve ou par un arbitre.

Dans le rôle de pointeur temporel, un tiers de confiance est censé apporter une preuve telle que le moment où la demande de pointage temporel a été reçue.

Dans le rôle de surveillant, un tiers de confiance contrôle l'action ou l'événement et est censé donner la preuve de ce qui a été surveillé.

Dans le rôle de certificateur de clé, un tiers de confiance fournit des certificats de non-répudiation associés à un générateur de preuve afin de garantir la validité d'une clé publique à utiliser pour des fins de non-répudiation.

Dans le rôle de distributeur de clés, un tiers de confiance fournit des clés aux générateurs de preuve et/ou aux vérificateurs de preuve. Il peut aussi imposer des contraintes à l'utilisation des clés, en particulier lorsque des techniques symétriques sont utilisées.

Dans le rôle de producteur de signature, un tiers de confiance est censé fournir une preuve sous la forme d'une signature numérique au nom du sujet de preuve.

Dans le rôle de vérificateur de preuve, un tiers de confiance vérifie la preuve à la demande d'une autre entité.

Dans le rôle de vérificateur de signature, un tiers de confiance est censé vérifier une preuve, pour le compte d'un utilisateur de preuve, sous la forme d'une signature numérique.

NOTE – Le rôle de producteur de signature est un cas particulier du rôle de producteur de preuve. Le rôle de vérificateur de signature est un cas particulier du rôle de vérificateur de preuve.

Dans le rôle de notaire, un tiers de confiance fournit une assurance au sujet des propriétés des données communiquées entre deux ou plus de deux entités, telles que l'intégrité, l'origine, l'heure ou la destination des données.

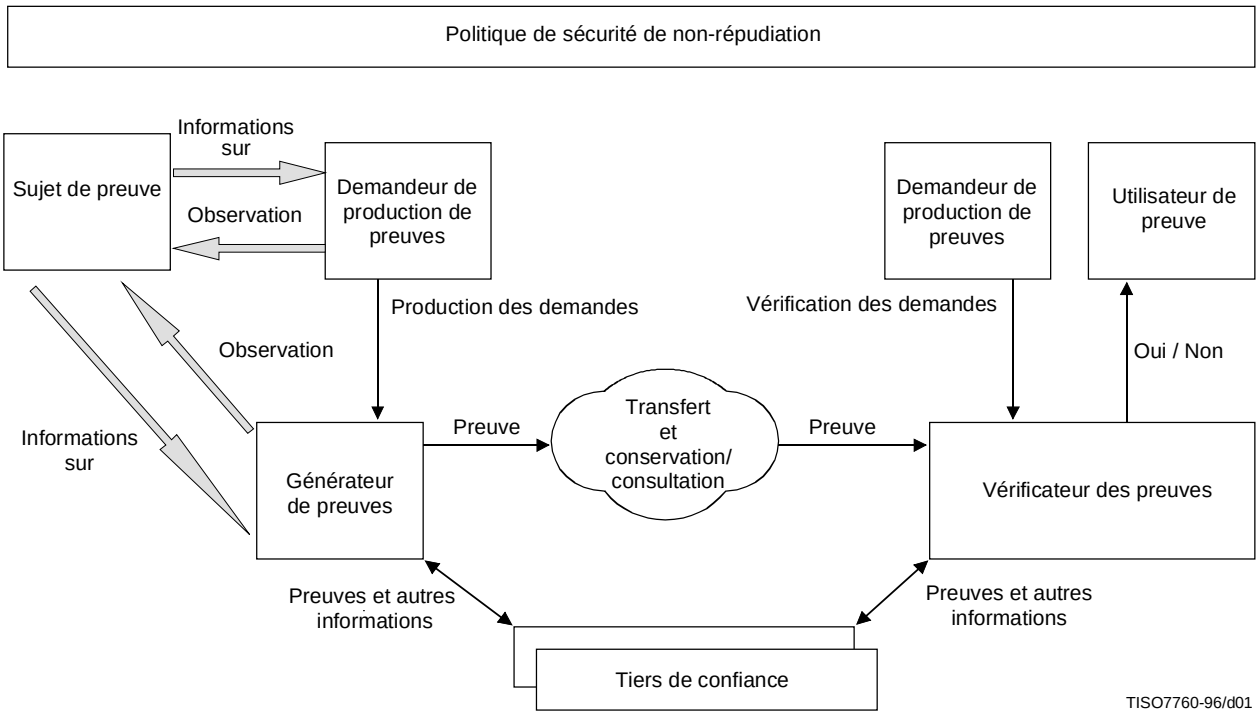
Dans le rôle d'autorité de remise, un tiers de confiance entre en interaction avec le destinataire prévu des données et essaye de les lui remettre. Il fournit ensuite la preuve que les données ont été remises, qu'elles n'ont pas été remises ou que la remise a été tentée mais qu'aucune confirmation de réception n'a été reçue. Dans ce dernier cas, l'utilisateur de la preuve ne peut pas déterminer si les données ont été reçues par le destinataire prévu ou non.

5.3 Phases de la non-répudiation

La non-répudiation se compose de quatre phases distinctes:

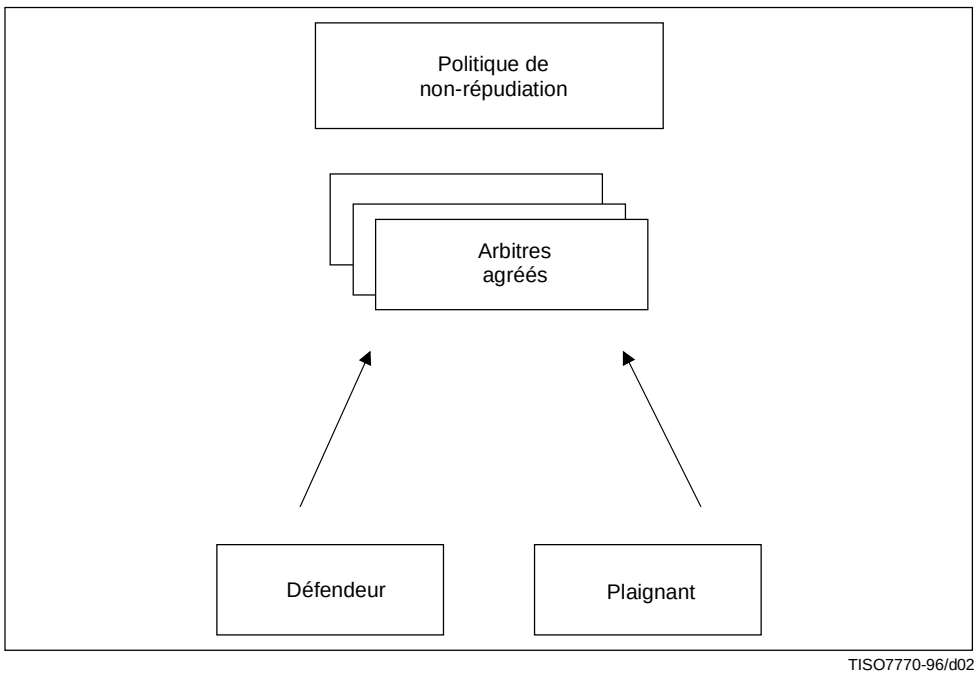
- la production des preuves;
- le transfert, la conservation et la consultation des preuves;
- la vérification des preuves;
- la résolution des litiges.

La Figure 1 montre les trois premières phases. La Figure 2 montre la quatrième phase.



NOTE – Cette figure, donnée à titre d'illustration, n'est pas définitive.

Figure 1 – Entités impliquées dans les phases de production, de transfert, de consultation/conservation et de vérification des preuves



NOTE – Cette figure, donnée à titre d'illustration, n'est pas définitive.

Figure 2 – Phase de résolution des litiges lors d'un processus de non-répudiation

5.3.1 Production des preuves

Dans cette phase, le demandeur de production de preuve demande au générateur de preuve de produire la preuve d'un événement ou d'une action. Une entité dont la participation à cet événement ou à cette action est établie par la preuve est appelée «*sujet de preuve*». Différents groupages de ces entités sont possibles: un sujet de preuve et un producteur de preuve peuvent être la même entité, de même que le sujet de preuve, le demandeur de production de preuve et le générateur de preuve; le demandeur de production de preuve et le tiers de confiance; le générateur de preuve et le tiers de confiance; et le demandeur de production de preuve, le générateur de preuve et le tiers de confiance. Selon le type de service de non-répudiation, la preuve peut être produite par le sujet de preuve, éventuellement en conjonction avec les services d'un tiers de confiance, ou par celui-ci uniquement.

NOTE – En fonction du contexte du service de non-répudiation, les preuves applicables comprendront normalement l'identité des entités mises en jeu, les données, l'heure et la date. D'autres informations pourront être ajoutées, telles que: le mode de transfert (par exemple communication OSI, conservation et consultation d'une base de données); l'emplacement des entités en cause; l'identificateur distinctif; et le «propriétaire»/créateur des données.

5.3.2 Transfert, conservation et consultation des preuves

Dans cette phase, la preuve est transférée d'une entité à une autre ou à destination/en provenance d'une mémoire (voir la Figure 1).

5.3.3 Vérification des preuves

Dans cette phase, la preuve est contrôlée par un vérificateur de preuve à la demande d'un utilisateur de preuve. L'objet de cette phase est de donner à un utilisateur de preuve l'assurance que la preuve fournie sera vraiment suffisante en cas d'apparition d'un litige. Des services de tiers de confiance peuvent y être ajoutés afin de donner des informations permettant de vérifier la preuve. Une même entité peut assumer les rôles d'utilisateur de preuve et de vérificateur de preuve.

5.3.4 Résolution des litiges

Dans la phase de résolution des litiges, un arbitre a la responsabilité de résoudre les litiges entre parties. Les parties en litige sont parfois désignées par les termes de «*plaignant*» et de «*défendeur*». La phase de résolution des litiges est décrite dans la Figure 2.

Lorsque l'arbitre résout des litiges, il recueille des preuves auprès des parties en litige et/ou des tiers de confiance. Le procédé utilisé par un arbitre pour résoudre des litiges est hors du domaine d'application de la présente Recommandation | Norme internationale.

Cette phase n'est pas toujours nécessaire. Si toutes les parties intéressées conviennent qu'un événement ou une action s'est produit (ou ne s'est pas produit), il n'y a aucun litige à résoudre. Par ailleurs, même si un litige s'est produit, il peut parfois être résolu directement entre les parties sans devoir faire appel à un arbitre. Par exemple, si l'une des parties au litige est honnête mais s'est trompée, elle peut se rendre compte de son erreur lorsqu'on lui montre la preuve de l'autre partie.

Bien que cette phase ne soit pas toujours nécessaire dans chaque instance du service de non-répudiation, tous les mécanismes de non-répudiation doivent prendre en charge la phase de résolution des litiges. En d'autres termes, ils doivent permettre la résolution des litiges lorsque ceux-ci se produisent.

5.4 Formes du service de non-répudiation

Il existe de nombreuses formes du service de non-répudiation, parmi lesquelles on relève fréquemment celle du service de non-répudiation associé au transfert de données.

Le transfert d'un message implique au moins deux entités, à savoir l'expéditeur et le destinataire. D'éventuels litiges concernant l'événement sont par exemple les suivants:

- litiges dans lesquels la participation de l'expéditeur à l'événement est contestée; par exemple, l'expéditeur supposé fait valoir que le message a été fabriqué de toutes pièces par le destinataire ou par un usurpateur d'identité malveillant;
- litiges dans lesquels la participation du destinataire à l'événement est contestée; par exemple, le destinataire supposé fait valoir soit que le message n'a pas été envoyé, soit qu'il a été perdu en transit ou qu'il n'a été reçu que par un usurpateur d'identité malveillant.

Pour la messagerie, les services de non-répudiation peuvent être classés selon le type de litige qu'ils peuvent contribuer à résoudre.

Le transfert de messages d'un expéditeur à un destinataire peut être considéré comme étant une séquence d'événements distincts:

- la transmission du message de l'expéditeur à un agent de transfert;
- la transmission du message d'un agent de transfert à un autre (si plusieurs agents de transfert sont impliqués);
- la transmission du message d'un agent de transfert au destinataire.

Pour chacun de ces événements, il existe des formes du service de non-répudiation qui apportent des preuves concernant ces événements. Les services additionnels de non-répudiation ci-après sont donc répertoriés:

- le service de non-répudiation avec preuve de soumission est utilisé pour s'assurer contre un faux déni, par un agent de transfert, de l'acceptation d'un message à transmettre (en provenance de l'expéditeur ou d'un autre agent de transfert);
- le service de non-répudiation avec preuve de transport est utilisé pour s'assurer contre un faux déni, par un agent de transfert, de la transmission d'un message (soit au destinataire soit à un autre agent de transfert).

NOTE – Les services de non-répudiation avec preuve de soumission et de non-répudiation avec preuve de transport n'apportent pas de preuve qu'une entité est responsable du message ou a compris l'information contenue dans le message.

5.5 Exemples de preuve OSI de non-répudiation

Selon les services OSI de non-répudiation invoqués, des formes particulières de preuve sont requises pour chaque type d'événement ou d'action, comme illustré ci-dessous.

5.5.1 Non-répudiation d'origine

La preuve doit comprendre les éléments suivants (dont chacun peut être signé ou notarié):

- l'identificateur distinctif de l'expéditeur;
- les données envoyées, ou une empreinte numérique de ces données.

La preuve peut également comprendre les éléments suivants:

- l'identificateur distinctif du destinataire;
- la date et l'heure de l'envoi des données.

5.5.2 Non-répudiation de remise

La preuve doit comprendre les éléments suivants (dont chacun peut être signé ou notarié):

- l'identificateur distinctif du destinataire;
- les données envoyées, ou une empreinte numérique de ces données.

La preuve peut également comprendre les éléments suivants:

- l'identificateur distinctif de l'expéditeur;
- la date et l'heure de la réception des données.

Lorsqu'une autorité de remise est utilisée, la preuve peut également comprendre les éléments suivants (dont chacun peut être signé ou notarié):

- l'identificateur distinctif de l'autorité de remise;
- la date et l'heure de la première tentative de remise par l'autorité de remise;
- la date et l'heure d'obtention du signal «prêt à recevoir» en provenance du destinataire;
- la date et l'heure d'exécution de la remise par l'autorité de remise;
- la date et l'heure auxquelles l'autorité de remise n'a pas été en mesure d'effectuer la remise;
- la cause probable des conditions de non-remise (par exemple rupture de la voie de communication);
- une indication des prescriptions de traitement qui ont été satisfaites lors de la remise du message.

6 Politiques de non-répudiation

Une politique de non-répudiation peut comprendre les règles suivantes:

- règles pour la production de preuves, par exemple spécifications des classes d'activité pour lesquelles une preuve de non-répudiation doit être produite; spécifications des tiers de confiance à utiliser pour produire la preuve; les rôles que ces tiers de confiance peuvent jouer; les procédures que les entités doivent suivre lors de la production des preuves;
- règles pour la vérification des preuves, par exemple spécifications des tiers de confiance dont les preuves sont acceptables; formes de preuve qui seront acceptées de la part de chaque tiers de confiance;

- règles pour la conservation des preuves, par exemple les moyens à utiliser pour assurer l'intégrité des preuves conservées;
- règles pour l'utilisation des preuves, par exemple spécification des fins auxquelles les preuves peuvent être utilisées;

  NOTE – Avec certains mécanismes de non-répudiation, il est parfois difficile d'empêcher un usage non autorisé des preuves.
- règles pour l'arbitrage, par exemple la spécification d'arbitre(s) agréé(s) pouvant régler un litige.

Chacun de ces ensembles de règles peut être défini par une autorité différente. Par exemple, les règles de production de preuves peuvent être définies par le propriétaire d'un système, alors que les règles d'arbitrage peuvent être définies par la loi du pays dans lequel le système existe.

Si différentes parties de la politique ne sont pas cohérentes, le service de non-répudiation peut ne pas fonctionner correctement, par exemple en autorisant, au cours de la phase de résolution des litiges, la réussite du déni d'un événement qui s'est réellement produit.

La politique de non-répudiation peut elle-même être utilisée par l'arbitre lors de la résolution d'un litige. Par exemple, l'arbitre peut se référer à la politique de non-répudiation pour déterminer si les règles de production de preuve ont été observées.

Les politiques de sécurité peuvent être explicitement déclarées, ou être définies implicitement par les implémentations. Une déclaration explicite de la politique de non-répudiation (par exemple un document en langage naturel) peut aider à détecter des conflits entre différentes parties de la politique. Elle peut également aider l'arbitre.

Les politiques de non-répudiation traitent également des cas dans lesquels la preuve a fait l'objet d'une divulgation forcée ou dans lesquels les clés utilisées pour produire la preuve ont fait l'objet d'une divulgation forcée ou d'une révocation.

Les politiques de non-répudiation pour interactions entre domaines de sécurité peuvent être le résultat d'accords conclus entre domaines de sécurité indépendants ou peuvent être imposées par un super-domaine.

7 Informations et fonctionnalités

7.1 Informations

Les informations qui peuvent être utilisées pour résoudre un litige sont appelées *preuves*. Une preuve peut être conservée localement par un utilisateur de preuve ou être conservée par un tiers de confiance. Formes particulières de preuve: signatures numériques, enveloppes sécurisées et jetons de sécurité. Les signatures numériques sont utilisées avec les techniques de clé publique tandis que les enveloppes sécurisées et les jetons de sécurité sont utilisés avec les techniques de clé privée. Exemples d'informations pouvant constituer une preuve:

- identificateur de la politique de sécurité de non-répudiation;
- identificateur distinctif de l'expéditeur;
- identificateur distinctif du destinataire;
- signature numérique ou enveloppe sécurisée;
- identificateur distinctif du générateur de preuve;
- identificateur distinctif du demandeur de production de preuve;
- message ou empreinte numérique du message;

  NOTE – Lorsque l'empreinte numérique est utilisée à la place du message, un indicateur est requis pour identifier la méthode utilisée pour la description.
- identificateur du message;
- indication de la clé secrète nécessaire pour valider le jeton de sécurité;
- identification de la clé publique particulière qui est nécessaire pour valider la signature numérique (par exemple l'identificateur de l'autorité de certification et le numéro de série du certificat);
- identificateur distinctif du notaire, du tiers de confiance de pointage temporel, du tiers de confiance en ligne, etc.;
- identificateur unique pour la preuve;
- date et heure du dépôt ou de l'enregistrement de la preuve;
- date et heure de la production de la signature numérique ou du jeton de sécurité.

7.2 Fonctionnalités de non-répudiation

Ce paragraphe identifie un certain nombre de fonctionnalités de non-répudiation qui peuvent être utilisées pour produire, envoyer et valider des preuves ou pour les déposer auprès d'un tiers de confiance.

7.2.1 Fonctionnalités associées à la gestion de non-répudiation

Les activités associées à la gestion de la non-répudiation peuvent impliquer la distribution d'informations, de mots de passe ou de clés (au moyen de la gestion des clés), à des entités appelées à effectuer une non-répudiation. Ces activités peuvent impliquer l'utilisation d'un protocole entre entités communicantes et entre autres entités fournissant des services de non-répudiation. La gestion de non-répudiation peut aussi impliquer la révocation des clés utilisées pour produire les preuves.

Les fonctionnalités de gestion de non-répudiation permettent à un utilisateur d'obtenir, de modifier et de supprimer des informations qui sont nécessaires pour la fourniture du service de non-répudiation. En termes généraux, ces fonctionnalités sont les suivantes:

- installation d'informations de gestion;
- modification d'informations de gestion;
- suppression d'informations de gestion;
- énumération d'informations de gestion.

Les actions suivantes, associées à la gestion de non-répudiation, peuvent être requises à l'appui du service de non-répudiation:

- enregistrement de l'événement dans le journal d'audit;
- enregistrement des résultats de l'arbitrage en cas de litige;
- signalisation locale de l'événement;
- signalisation distante de l'événement.

L'action spécifique qui doit faire suite à chaque événement dépend de la politique de sécurité mise en œuvre.

7.2.2 Fonctionnalités associées aux opérations

7.2.2.1 Production des preuves

Cette fonctionnalité est utilisée pour produire des preuves. Ces preuves peuvent être générées directement par le sujet de preuve (sans faire intervenir un tiers de confiance), par un ou plusieurs tiers de confiance agissant pour le compte du sujet de preuve, ou par le sujet de preuve de concert avec un ou plusieurs tiers de confiance.

Les éléments susceptibles d'être introduits sont les suivants:

- la politique de non-répudiation;
- l'identificateur distinctif du sujet de preuve;
- l'identificateur distinctif du demandeur du service de non-répudiation;
- les données, ou une empreinte numérique des données;
- l'identificateur distinctif du tiers de confiance qui sera utilisé pour produire la signature numérique, le jeton de sécurité ou une autre preuve.

Les éléments susceptibles d'être produits sont les suivants:

- une preuve (par exemple une signature numérique ou un jeton de sécurité);
- l'identificateur distinctif du tiers de confiance qui a produit la signature numérique, le jeton de sécurité ou une autre preuve.

7.2.2.2 Production des pointeurs temporels

Cette fonctionnalité est utilisée pour produire des pointeurs temporels.

Les éléments susceptibles d'être introduits sont les suivants:

- l'identificateur distinctif de l'entité demandant le pointeur temporel;
- l'identificateur distinctif du tiers de confiance jouant le rôle de pointeur temporel;
- les données (par exemple message signé, accusé de réception) ou une signature numérique ou une empreinte numérique des données.

Les éléments susceptibles d'être produits sont les suivants:

- la contresignature calculée par le tiers de confiance;
- une identification de la méthode et/ou de l'algorithme cryptographique utilisé pour produire la contresignature (qui indique en corollaire si ce sont les données qu'on utilise, ou leur empreinte numérique);
- l'identificateur distinctif du service de pointage temporel;
- la date et l'heure de réception de la demande de pointage temporel;
- la date et l'heure de production de la contresignature;
- un message signé comportant un pointeur temporel et une empreinte numérique des données d'entrée.

7.2.2.3 Production de preuves notariées

Cette fonctionnalité est utilisée pour déposer des preuves auprès du tiers de confiance.

Les éléments susceptibles d'être introduits sont les suivants:

- l'identificateur distinctif du demandeur de production de preuve;
- la preuve (par exemple une signature numérique ou un jeton de sécurité);
- l'identificateur distinctif du générateur de preuve;
- l'identificateur distinctif de la politique de non-répudiation.

Les éléments susceptibles d'être produits sont les suivants:

- le numéro d'enregistrement de la preuve;
- la date et l'heure de l'enregistrement de preuve.

7.2.2.4 Validation de preuve

Cette fonctionnalité est utilisée pour valider une preuve.

Les éléments susceptibles d'être introduits sont les suivants:

- la preuve;
- l'identificateur distinctif du sujet de preuve;
- l'identificateur distinctif de l'utilisateur de preuve;
- l'identificateur de la clé à utiliser pour vérifier la preuve;
- une indication de l'usage prévu de la preuve (de manière qu'une évaluation puisse déterminer si la preuve est appropriée à cette fin dans le cadre de la politique de non-répudiation).

Les éléments susceptibles d'être produits sont les suivants:

- le résultat de la vérification (preuve valide ou invalide);
- l'identificateur distinctif du sujet de preuve;
- l'identificateur distinctif du générateur de preuve;
- l'identificateur distinctif du demandeur de vérification de preuve;
- l'identificateur distinctif du tiers de confiance qui a vérifié la signature numérique ou le jeton de sécurité;
- les données ou leur empreinte numérique.

7.2.2.5 Production de preuves pour les transferts de données par l'intermédiaire d'un tiers de confiance en ligne

Au lieu d'envoyer des données et/ou des accusés de réception directement entre un expéditeur et un destinataire, les données peuvent être transférées par l'intermédiaire d'un tiers de confiance, de manière que la preuve de non-répudiation puisse être assurée par le tiers de confiance. Cette fonctionnalité peut aussi être utilisée lorsque l'on craint qu'un destinataire puisse invoquer une panne de voie de communication pour dénier la remise des données.

Pour utiliser cette fonctionnalité, les éléments suivants doivent être présentés au tiers de confiance en ligne:

- les données;
- l'identificateur distinctif du destinataire.

En outre, les éléments suivants peuvent être présentés:

- une empreinte numérique des données;
- l'identificateur distinctif de l'expéditeur;
- une signature numérique;
- l'identificateur distinctif du tiers de confiance en ligne;
- la politique de non-répudiation.

Les éléments susceptibles d'être produits par le tiers de confiance en ligne sont les suivants:

- l'identificateur distinctif du tiers de confiance en ligne;
- l'identificateur distinctif du destinataire;
- le numéro d'enregistrement de la preuve;
- la date et l'heure de l'enregistrement;
- les données, ou leur empreinte numérique.

8 Mécanismes de non-répudiation

Le service de non-répudiation peut être fourni par l'intermédiaire de mécanismes tels que: signatures numériques, chiffrement, notarisation et intégrité des données, qui servent de base à d'autres services, comme le pointage temporel. Pour le service de non-répudiation, on peut utiliser des algorithmes cryptographiques aussi bien symétriques qu'asymétriques. Le service de non-répudiation peut faire appel à une combinaison de ces mécanismes et services, selon les besoins, afin de répondre aux prescriptions de sécurité de l'application en question.

Le présent article décrit les mécanismes qui peuvent être utilisés pour fournir le service de non-répudiation, ainsi que certaines des menaces auxquelles ces mécanismes sont exposés.

8.1 Non-répudiation au moyen d'un jeton de sécurité de tiers de confiance (enveloppe sécurisée)

Dans ce mécanisme, la preuve de non-répudiation se compose d'un jeton de sécurité, cacheté par une clé secrète, connue seulement d'un tiers de confiance. Celui-ci produit le jeton de sécurité à la demande du demandeur de production de preuve. Il peut par la suite en faire la vérification pour le compte de l'utilisateur de preuve ou pour l'arbitre. Dans ce cas, le tiers de confiance est le générateur de preuve et le vérificateur de preuve.

Un demandeur de production de preuve transmet au tiers de confiance les données (ou leur empreinte numérique) avec une demande de production d'un jeton de sécurité. Cette demande doit être protégée en termes d'intégrité (par exemple au moyen d'un cachet). Elle peut également être protégée en termes de confidentialité (par exemple au moyen d'un chiffrement). Les jetons de sécurité à protection d'intégrité sont parfois dénommés *enveloppes sécurisées*.

Les éléments susceptibles d'être introduits pour la production du jeton de sécurité sont les suivants:

- identification de la méthode et/ou de l'algorithme cryptographique utilisé pour assurer l'intégrité du jeton de sécurité;
- identification de la méthode et/ou de l'algorithme cryptographique utilisé pour assurer la confidentialité du jeton de sécurité;
- l'identificateur distinctif du sujet de preuve;
- l'identificateur distinctif du demandeur de production de preuve;
- la politique de non-répudiation applicable;
- la date et l'heure de l'événement ou de l'action;
- les données décrivant l'événement ou l'action.

Les éléments susceptibles d'être produits sont les suivants:

- un jeton de sécurité;
- la date et l'heure de la production du jeton de sécurité.

8.2 Non-répudiation au moyen de jetons de sécurité et de modules inviolables

Dans ce mécanisme, la preuve de non-répudiation se compose d'un jeton de sécurité, cacheté par une clé secrète qui est conservée à l'intérieur de modules cryptographiques inviolables que possèdent le générateur de preuve, le vérificateur de preuve et l'arbitre. Ces modules inviolables limitent les opérations qui peuvent être exécutées avec la clé secrète et empêchent que la valeur de la clé soit révélée à l'extérieur de son module.

Le module du générateur de preuve permet d'utiliser la clé secrète pour créer un jeton cacheté, alors que les modules possédés par le vérificateur de preuve et par l'arbitre ne permettent que la vérification des jetons. Toutes les parties impliquées doivent être assurées que les clés secrètes ont été installées correctement dans les modules cryptographiques inviolables, de manière que la même clé secrète ne puisse être utilisée que pour la production de preuves par une entité donnée et que pour la vérification de preuves par d'autres entités.

Si un litige apparaît, l'utilisateur de preuve présente le jeton cacheté à l'arbitre et fait valoir que ce jeton ne peut avoir été créé qu'au moyen du module du générateur de preuve, étant donné que les autres modules, contenant la même clé, n'ont pas la capacité de production de jetons de sécurité.

8.3 Non-répudiation au moyen d'une signature numérique

Dans ce mécanisme, la preuve de non-répudiation se compose d'une structure de données à signature numérique. La production de la signature fait appel à une clé de signature et la vérification de la signature fait appel à une clé de vérification.

Selon la politique de sécurité, un pointeur temporel peut être requis. Il peut être inclus dans la signature numérique fournie par une entité et/ou par un tiers de confiance agissant en tant qu'autorité de pointage temporel. Lorsque cette information n'est pas fournie par un tiers de confiance, les autres entités ne sont pas tenues de s'y fier. Si l'arbitre a besoin d'un pointeur temporel et/ou des informations contextuelles pour résoudre des litiges, cette information doit être obtenue de sources de confiance (par exemple des tiers de confiance).

Le vérificateur de preuve et l'arbitre doivent toujours être en mesure d'obtenir la clé de vérification afin de vérifier la preuve. Si l'on ne peut pas garantir que l'arbitre connaîtra la clé publique du générateur de preuve par d'autres moyens, la preuve doit aussi comporter un certificat de sécurité pour cette clé.

La signature numérique peut être créée par l'expéditeur/le destinataire ou être produite par un tiers de confiance jouant le rôle de producteur de signature.

Une signature numérique générée par le sujet de preuve est appelée signature numérique directe. Un mécanisme de signature numérique généré par un tiers de confiance pour le compte du sujet de preuve est appelé signature numérique médiate.

Les seules signatures numériques ne suffisent pas pour régler des litiges lorsque le certificat utilisé pour vérifier la signature a été révoqué. Pour résoudre de tels litiges, il est également nécessaire de fournir à l'arbitre des preuves au sujet de la révocation des certificats (par exemple des listes de révocation de certificats – CRL) montrant que le certificat était encore valide au moment de la production de la signature numérique. Ce mécanisme ne permet cependant pas le règlement de litiges lorsque le détenteur de la clé privée utilise une heure incorrecte, ou lorsqu'un attaquant compromet la clé privée qui a été utilisée pour produire la signature. Pour régler de tels litiges, il est nécessaire d'utiliser en outre une référence temporelle de confiance ou une contresignature issue d'un tiers de confiance jouant le rôle de pointeur temporel (voir l'Annexe E).

Un vérificateur de preuve peut utiliser un service d'annuaire pour obtenir des renseignements (comme des certificats de sécurité) nécessaires pour le processus de vérification. Le vérificateur de preuve doit toujours obtenir la clé publique du générateur de preuve. Cette clé peut être contenue dans un certificat de sécurité qui est conservé dans l'Annuaire. Plusieurs certificats de sécurité sont parfois requis. Pour garantir qu'un certificat est valide, il est aussi nécessaire de demander les certificats de révocation applicables et ce pour chaque autorité de certification qui apparaît dans un chemin de certification (voir la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Un utilisateur de preuve peut demander l'assistance d'un tiers de confiance qui joue le rôle de vérificateur de signature, afin de valider une signature numérique. Dans ce rôle, le tiers de confiance vérifie la relation entre le message original (ou, si elle est utilisée, l'empreinte numérique du message) et sa signature numérique.

Dans ce cas, le rôle du tiers de confiance est d'épargner à l'utilisateur de preuve la complexité du processus de vérification de signature et de conserver les résultats de demandes de vérification antérieures afin d'optimiser les réponses à d'ultérieures demandes de vérification. A cette fin, le tiers de confiance peut avoir besoin d'une certaine interaction avec un Annuaire. Le tiers de confiance faisant office de vérificateur de signature est censé détenir la clé publique d'au moins une autorité de certification. Le tiers de confiance tient également compte des relations de confiance qui existent entre différentes autorités de certification.

8.4 Non-répudiation au moyen de pointages temporels

Lorsqu'une référence temporelle habilitée est nécessaire et que l'on ne peut pas se fier aux signaux d'horloge fournis par l'entité qui produit la signature numérique ou le jeton de sécurité, il faut se fonder sur un tiers de confiance pour fournir le pointage temporel. Celui-ci peut servir à confirmer qu'un message a été signé avant la négociation de la clé de signature et donc que le message n'est pas un faux. Dans le rôle de pointeur temporel, le tiers de confiance fournira une signature numérique ou un jeton de sécurité permettant de déterminer le moment où la demande a été reçue. Le pointage temporel peut être demandé par le générateur de preuve, par le demandeur de service de non-répudiation, par l'utilisateur de preuve ou par le vérificateur de preuve.

Le pointage temporel ajoute aux données l'heure et la date ainsi qu'un cachet ou une signature numérique. Le pointage temporel ne nécessite pas l'authentification de l'entité qui a demandé le pointeur temporel. Le vérificateur de preuve doit déterminer si les marqueurs temporels sont compris dans une gamme acceptable en fonction de la politique de sécurité.

Le pointage temporel peut être combiné aux rôles de production de signature et de production de jeton. Si l'entité qui produit la signature numérique y ajoute un signal d'horloge fiable et confirmé, une contresignature n'est pas forcément requise.

8.5 Non-répudiation au moyen d'un tiers de confiance en ligne

La fonctionnalité de non-répudiation au moyen d'un tiers de confiance en ligne peut être demandée explicitement par un événement particulier ou une action particulière ou être fournie implicitement. Le tiers de confiance en ligne agit alors comme intermédiaire dans toutes les interactions pour lesquelles le service de non-répudiation est demandé. Il peut également fournir une preuve à un utilisateur de preuve (tel qu'un arbitre). Le tiers de confiance en ligne retransmettra toujours les données et surveillera l'événement ou l'action.

Le tiers de confiance est censé conserver des enregistrements pour la future résolution de litiges. Les données (ou leur empreinte numérique) peuvent devenir des preuves si elles sont conservées par le tiers de confiance.

8.6 Non-répudiation au moyen d'un notaire

Un mécanisme de notarisation fournit une assurance au sujet des propriétés de données communiquées entre deux ou plus de deux entités, par exemple en termes d'intégrité, d'origine, de temps et de destination. Un notaire est habilité par les entités impliquées à détenir les informations requises pour fournir des assurances de manière contrôlable et à conserver des enregistrements pour la future résolution de litiges. Les mécanismes de signature numérique, de chiffrement et d'intégrité peuvent être utilisés, selon le cas, à l'appui du service fourni par le notaire.

Dans le rôle de production de preuve, le notaire enregistrera des preuves afin de garantir les propriétés des données. En outre, un numéro d'enregistrement peut être utilisé afin d'identifier cette preuve.

Dans le rôle de vérificateur de preuve, le notaire confirme la validité de la preuve.

8.7 Menaces pouvant affecter la non-répudiation

Aucun mécanisme de non-répudiation n'est complètement invulnérable à toutes les menaces. Un mécanisme qui met en œuvre un tiers de confiance peut ne pas être sûr si ce tiers n'a pas le comportement qu'il est censé avoir. Cela peut se produire soit à la suite d'une panne fortuite soit à la suite d'une attaque provenant de l'intérieur. Les conséquences de cette menace peuvent être importantes mais ne seront pas analysées plus profondément dans la présente Recommandation | Norme internationale. Les mécanismes de non-répudiation varient selon les conséquences de l'inconduite du tiers de confiance et selon la facilité avec laquelle un tiers de confiance peut provoquer des pannes de protocole. Une évaluation doit être faite pour déterminer les menaces qui sont possibles et celles qui ont des conséquences importantes dans un environnement particulier, afin de sélectionner des mécanismes contenant le risque total dans des limites acceptables. On trouvera ci-après quelques exemples de ces menaces, ainsi que de contre-mesures possibles.

8.7.1 Divulgation forcée de clés

8.7.1.1 Divulgation forcée de la clé de production de preuve d'une entité

Dans la période qui s'écoule entre la divulgation forcée d'une clé et la détection de cette divulgation par le propriétaire légitime de cette clé, le risque existe qu'un assaillant fasse usage de la clé divulguée pour produire une preuve que l'utilisateur de preuve acceptera comme étant valide. Le mécanisme de non-répudiation ne peut pas se rétablir à la suite d'un dommage causé par une telle utilisation frauduleuse d'une clé de production de preuve. Il est toutefois possible de déterminer l'étendue du dommage en faisant appel à une autorité de production de preuve (par exemple une autorité de

production de signature) qui pourra ensuite conserver un journal d'audit des preuves produites. Ce journal permettra de découvrir quelle preuve a été produite et à quel moment. Il est également souhaitable de faire connaître aussi largement que possible le fait que la clé a fait l'objet d'une utilisation frauduleuse. Mais il ne sera pas toujours possible d'atteindre tous les destinataires qui ont reçu des preuves construites au moyen de la clé de production divulguée.

Dès que cette divulgation de clé est détectée par le propriétaire légitime de cette clé, la clé de production doit être révoquée. Si cette clé est privée, il faut révoquer le certificat de clé publique correspondant, ce qui peut se faire au moyen des listes de révocation de certificat définies dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Ce n'est cependant pas suffisant, car cela n'empêche pas un emploi frauduleux de la clé. Les moyens permettant de contrer cette menace consistent par exemple à faire appel à un sujet de preuve. L'utilisation de signatures numériques passant par un intermédiaire ou de contresignatures issues d'une autorité de pointage temporel peut protéger contre ce type de menace. Dans ce dernier cas, la politique de non-répudiation spécifie que la preuve n'est valide que si elle est contresignée correctement par une autorité de pointage temporel (voir l'Annexe E).

La divulgation de clé peut également être délibérée. Si la politique de non-répudiation spécifie qu'un sujet de preuve ne sera pas tenu responsable pour l'emploi frauduleux de sa clé entre l'instant où celle-ci est divulguée et l'instant où cette divulgation est détectée, le sujet de preuve pourra tirer avantage de cette clause pour revendiquer la divulgation de sa clé et pour ensuite répudier une action ou un événement qui a effectivement eu lieu. Il est possible de contrer cette menace en définissant un délai maximal autorisé avant de signaler la divulgation d'une clé. Selon cette politique, si un utilisateur de preuve omet de déclarer la divulgation de sa clé dans ce délai, le sujet de preuve est tenu pour responsable des éventuelles conséquences de l'utilisation frauduleuse de sa clé. Les vérificateurs de preuve peuvent donc, avant d'accepter une quelconque preuve, s'assurer que le délai imparti pour la déclaration d'une divulgation de clé est arrivé à expiration.

8.7.1.2 Divulgation d'une clé de production de preuve d'un tiers de confiance

Lorsque la divulgation d'une clé de tiers de confiance a été détectée, cette clé doit être révoquée. Si cette clé est privée, il faut révoquer le certificat de clé publique correspondant, ce qui peut se faire au moyen des listes de révocation de certificat définies dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Pour traiter une preuve déjà produite au moyen de la clé (éventuellement) divulguée, il est nécessaire que le tiers de confiance conserve un journal d'audit de chaque utilisation de sa clé. Si celle-ci est divulguée, ce journal d'audit pourra servir pour le règlement des litiges.

8.7.1.3 Substitution de la clé de vérification de preuve d'une entité

Par cette menace, un utilisateur/vérificateur de preuve est faussement induit à croire qu'il possède une preuve valide. Cependant, lorsqu'un litige nécessitant un arbitrage se produit, l'on découvre que la preuve est invalide. Dans ce cas, l'utilisateur de preuve est perdant parce qu'il a agi de bonne foi sur la base d'une preuve apparemment valide, mais constatée comme fausse par l'arbitre. Les moyens permettant de contrer cette menace sont par exemple l'emploi de procédures renforcées pour s'assurer que la bonne entité est associée à la bonne clé de vérification. Si une substitution se produit, la fausse clé de vérification doit être supprimée dès que la substitution est détectée.

8.7.1.4 Substitution de la clé de vérification de preuve d'un tiers de confiance

Si la clé de vérification est une clé publique utilisée par un tiers de confiance pour vérifier directement une preuve, ce tiers peut être faussement induit à accepter une preuve falsifiée par falsification de ce qui transmet la clé de vérification à l'arbitre (par exemple des documents imprimés, une chaîne de certificats). Un exemple particulier de cette menace est la substitution par un assaillant de la copie d'arbitre d'une clé publique.

Lorsqu'une attaque de ce type a été détectée, il y a lieu de signaler la substitution aussi largement que possible. Mais il convient de noter qu'il ne sera pas toujours possible d'atteindre tous les utilisateurs de preuve qui ont utilisé une preuve pouvant avoir été vérifiée au moyen de la clé substituée. Avant de signaler la substitution, il est possible de déterminer quelle preuve a été vérifiée en faisant appel à une autorité de vérification de preuve (comme une autorité de vérification de signature) qui pourra alors conserver un journal d'audit des preuves vérifiées. Il sera ainsi possible de savoir quelle preuve a été vérifiée avant la signalisation de substitution, et quelle preuve a été vérifiée après.

Si la clé de vérification est une clé publique employée par des utilisateurs de preuve pour vérifier directement des certificats, il y a lieu de changer cette clé dès que la substitution est détectée.

8.7.2 Compromission de preuve

Des informations acceptables à un moment comme preuve peuvent cesser d'être acceptables. De telles informations sont appelées *preuve compromise*.

8.7.2.1 Modification ou destruction de preuve sans autorisation

Dans ce cas, l'action ou l'événement s'est effectivement produit mais la partie ayant intérêt à répudier l'événement s'arrange pour modifier ou détruire les preuves conservées. Cette partie peut ensuite répudier sans opposition un événement qui, en fait, a eu lieu. On peut contrer cette menace en employant des mécanismes de sécurité appropriés, empêchant la modification ou la destruction des preuves (comme un stockage redondant). L'utilisation d'un tiers de confiance pour mémoriser des preuves peut apporter un complément de protection contre cette menace car les supports de stockage conservés par un tiers de confiance sont souvent mieux protégés que ceux de l'utilisateur de preuve.

8.7.2.3 Destruction ou invalidation de preuves

Dans cette menace, les preuves mémorisées par le tiers de confiance sont détruites. Cette menace peut apparaître si le tiers de confiance n'est pas suffisamment attentif et n'a pas pris les dispositions adéquates pour la sauvegarde. On peut contrer cette menace en faisant appel à des mécanismes de non-répudiation dans lesquels toutes les preuves requises pour résoudre des litiges sont mémorisées par l'utilisateur de preuve. Celui-ci peut ensuite s'assurer que les preuves ne sont pas détruites, même si un tiers de confiance est malhonnête ou négligent.

8.7.3 Falsification de preuve

8.7.3.1 Falsification de preuve par un intrus

Dans ce cas, un événement contesté ne s'est pas produit, mais un intrus pénètre dans le système et crée une fausse preuve que l'événement s'est produit. Ce cas peut se présenter lorsqu'un notaire est impliqué. Des mécanismes cryptographiques peuvent être utilisés pour protéger des preuves mémorisées contre la création frauduleuse ou la modification par un intrus.

8.7.3.2 Fausse vérification de preuve

Dans les mécanismes où un tiers de confiance est utilisé pour vérifier des preuves, la menace existe que ce tiers dise à l'utilisateur de preuve qu'il a validé la preuve mais que celle-ci soit en fait invalide. En cas de litige, l'utilisateur de la preuve sera dans l'impossibilité de convaincre l'arbitre que l'événement contesté s'est produit. On peut se prémunir contre cette menace en faisant appel à un mécanisme de non-répudiation dans lequel le vérificateur de preuve peut vérifier la preuve directement, sans faire appel à un tiers de confiance.

8.7.3.3 Falsification de preuve par un tiers de confiance

Dans cette menace, un tiers de confiance peut créer une preuve frauduleuse pour un événement qui ne s'est jamais produit. Si ce tiers a la confiance de l'arbitre, celui-ci acceptera la preuve falsifiée et sera donc induit frauduleusement à prendre une décision incorrecte. On peut se prémunir contre cette menace en faisant appel à un mécanisme de non-répudiation dans lequel il est difficile aux tiers de confiance de falsifier des preuves, ou en s'assurant que ces tiers sont dignes de confiance et bien placés pour mériter cette confiance. En général, il est difficile de fournir des preuves irréfutables quant à la fiabilité d'une entité.

9 Interactions avec d'autres services et mécanismes de sécurité

Cet article décrit la façon dont d'autres services de sécurité peuvent être utilisés pour prendre en charge le service de non-répudiation. L'utilisation du service de non-répudiation pour prendre en charge d'autres services de sécurité n'est pas discutée ici.

9.1 Authentification

Lorsqu'elles interagissent avec un tiers de confiance, les entités peuvent avoir besoin de prouver leur identité au moyen d'un service d'authentification (légitimation). Des échanges ultérieurs pourront devoir être assurés au moyen d'un service d'authentification d'origine des données. Par exemple, lorsqu'un tiers de confiance est utilisé dans le rôle de producteur de signature, il peut être appelé à authentifier le sujet de preuve avant de produire une signature.

9.2 Contrôle d'accès

Un service de contrôle d'accès peut être utilisé pour garantir que les informations conservées ou le service offert par un tiers de confiance ne sont communiqués qu'à des entités autorisées.

9.3 Confidentialité

Les services de confidentialité peuvent être requis pour protéger les données contre une divulgation non autorisée (y compris, dans certains cas, une divulgation non autorisée par tiers de confiance ou à tiers de confiance) ainsi que pour protéger les parties contre une divulgation non autorisée de preuves.

9.4 Intégrité

Des services d'intégrité seront requis pour assurer l'intégrité des preuves.

Dans le cas du service de non-répudiation avec preuve d'origine ou du service de non-répudiation avec preuve de remise, l'intégrité des données doit également être assurée de manière que les données transférées entre un expéditeur et un destinataire ne puissent pas être modifiées sans détection.

9.5 Audit

Un utilisateur de preuve peut utiliser la fonction d'enregistrement d'audit pour conserver des preuves pouvant être utilisées en cas de litige ultérieur.

Un notaire ou un tiers de confiance en ligne peut utiliser la fonction d'enregistrement d'audit pour consigner le contenu, l'origine, la destination et l'heure des messages.

9.6 Gestion des clés

Un service de gestion des clés peut être utilisé afin de fournir des clés pouvant servir à la production et à la vérification de preuves. Le service de gestion de clés peut être appelé à fournir des clés pour la vérification des preuves, même si la clé correspondante, utilisée pour la production des preuves, a cessé d'être valide ou disponible.

Annexe A

Non-répudiation dans le modèle de référence de base OSI

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

A.1 Non-répudiation avec preuve d'origine

Le service de non-répudiation avec preuve d'origine donne au destinataire des données la preuve de l'origine de celles-ci. Ce service a pour objet de protéger contre toute tentative de l'expéditeur de nier faussement l'envoi des données ou de leur contenu. Cela peut être réalisé lorsque le générateur de preuves (habituellement l'expéditeur des données mais éventuellement un tiers de confiance) remet au vérificateur de preuve (habituellement le destinataire des données mais éventuellement une partie représentant celui-ci) la preuve que les données ont été envoyées par l'expéditeur.

Lorsqu'un mécanisme de signature est utilisé, la preuve est une signature numérique ou une empreinte digitale numérique des données. La non-répudiation avec preuve d'origine dépend d'un mécanisme préalablement convenu pour la fourniture de preuves validées. Ce mécanisme comporte les phases suivantes:

1) le demandeur du service de non-répudiation produit une signature pour les données ou obtient du notaire une signature et l'ajoute aux données;
2) la preuve est communiquée à l'utilisateur de preuve;
3) en cas de litige, les données et la preuve sont produites par l'utilisateur de preuve; l'arbitre vérifie la concordance entre données et preuve.

A.2 Non-répudiation avec preuve de remise

Le service de non-répudiation avec preuve de remise donne à l'expéditeur des données la preuve de la remise de celles-ci. Ce service protège contre toute tentative ultérieure du destinataire de nier faussement avoir reçu les données ou leur contenu. Cela peut être réalisé lorsque le générateur de preuves (habituellement le destinataire des données mais parfois aussi un tiers de confiance) remet au vérificateur de preuve (habituellement l'expéditeur des données mais parfois aussi une partie représentant l'expéditeur, ou un tiers de confiance) la preuve que les données ont été remises.

Ce service dépend du renvoi, par le destinataire des données, d'un accusé de réception contenant la preuve. Cet accusé de réception contiendra la confirmation de réception sous la forme d'une signature numérique sur le message original (ou d'une empreinte digitale numérique du message original) au moment de la réception.

Lorsqu'un mécanisme de signature est utilisé, un accusé de réception signé est requis comme preuve.

On peut considérer ce service selon deux cas de figure, selon qu'un tiers de confiance, jouant le rôle d'autorité de remise, est ou non impliqué dans la prise en charge de ce service.

Annexe B

Description des fonctionnalités de non-répudiation

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

<table>
<tr><td colspan="2" rowspan="2">Description des fonctionnalités de sécurité</td><td rowspan="2">Elément</td><td colspan="4">Entité: sujet de preuve, générateur de preuve, vérificateur de preuve, utilisateur de preuve, tiers de confiance de non-répudiation, arbitre</td></tr>
<tr><td colspan="4">Objet informationnel: preuve</td></tr>
<tr><td colspan="2"></td><td colspan="5">But de l'entité: collecter, conserver, communiquer et valider des preuves irréfutables</td></tr>
<tr><td rowspan="7">ACTIVITÉ</td><td>Entité</td><td colspan="5">Tiers de confiance, autorité de sécurité</td></tr>
<tr><td>Fonction</td><td colspan="5">(non définie)</td></tr>
<tr><td>Activité associée à la gestion</td><td colspan="5">– installer
– modifier
– supprimer
– énumérer</td></tr>
<tr><td>Entité</td><td>Sujet de preuve</td><td>Destinataire</td><td>Tiers de confiance de non-répudiation</td><td>Arbitre</td></tr>
<tr><td>Fonction</td><td>(non définie)</td><td>(non définie)</td><td>(non définie)</td><td>(non définie)</td></tr>
<tr><td>Activité associée aux opérations</td><td>– produire des preuves
– produire des preuves notariées</td><td>– produire des preuves
– produire des preuves notariées</td><td>– produire des pointeurs temporels
– transfert via tiers de confiance</td><td>(non définie)</td></tr>
<tr><td rowspan="3">INFORMATION</td><td>Elément de données d'entrée/sortie géré par SDA</td><td colspan="5">– Informations de gestion (par exemple mots de passe ou clés)
– Type d'information
– Politique de non-répudiation</td></tr>
<tr><td>Type d'information utilisé en exploitation</td><td colspan="5">– Preuve
– Signature numérique
– Jeton de sécurité
– Certificat de sécurité
– Pointeur temporel</td></tr>
<tr><td>Information de commande</td><td colspan="5">Enregistrement de l'événement dans le journal d'audit ainsi que des résultats d'arbitrage de litige; indication de la relation entre entités</td></tr>
</table>

Annexe C

Non-répudiation dans les systèmes en mode différé

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

Dans les systèmes en mode différé, un message est transféré entre son expéditeur et son destinataire par un ou plusieurs intermédiaires, appelés *agents de transfert*. Dans de tels systèmes, la transmission d'un message implique non seulement la communication entre l'expéditeur et le destinataire, mais aussi la communication entre l'expéditeur et un agent de transfert, la communication entre le destinataire et un agent de transfert, et la communication entre agents de transfert. Le service de non-répudiation peut être appliqué séparément à chacune des étapes du transport d'un message jusqu'à sa destination finale.

Le service de *non-répudiation avec preuve d'origine* protège contre un faux déni d'envoi d'un message ou de son contenu par l'expéditeur. Les preuves réunies par ce service peuvent être utilisées soit par le destinataire soit par les agents de transfert.

Le service de *non-répudiation avec preuve de remise* protège contre un faux déni de réception d'un message ou de son contenu par le destinataire. Les preuves réunies par ce service peuvent être utilisées soit par l'expéditeur soit par les agents de transfert.

Le service de *non-répudiation avec preuve de soumission* est utilisé pour protéger contre un faux déni, par un agent de transfert, d'avoir accepté un message à transmettre (provenant soit de l'expéditeur soit d'un autre agent de transfert). Cet expéditeur ou ces autres agents de transfert peuvent utiliser les preuves réunies par ce service.

Le service de *non-répudiation avec preuve de transport* est utilisé pour protéger contre un faux déni, par un agent de transfert, d'avoir transmis un message (soit au destinataire soit à un autre agent de transfert). L'expéditeur est l'utilisateur des preuves réunies par ce service.

Le service de *non-répudiation avec preuve de transfert* est utilisé pour protéger contre un faux déni, par un agent de transfert, d'avoir accepté la responsabilité de remettre un message. Ce service est utilisé lorsque plusieurs agents de transfert sont impliqués dans la remise d'un message. Lorsque le premier agent de transfert qui a accepté le message le transmet au deuxième agent de transfert, celui-ci peut donner au premier la preuve qu'il a accepté la responsabilité du message. Lorsque plus de deux agents de transfert sont impliqués, ce service peut également être utilisé entre le deuxième et le troisième agent, et ainsi de suite.

L'utilisation de ces différentes formes du service de non-répudiation est résumée dans le tableau suivant:

Nom du service	Protection contre	Utilisé par
Preuve d'origine	expéditeur	destinataire, agent de transfert
Preuve de soumission	agent de transfert	expéditeur
Preuve de transport	agent de transfert	expéditeur
Preuve de transfert	agent de transfert	agent de transfert
Preuve de remise	destinataire	expéditeur, agent de transfert

Ces formes additionnelles du service de non-répudiation (avec preuve de soumission et preuve de transport) peuvent être fournies par visibilité du système selon différents niveaux de granularité puis par utilisation de mécanismes fournissant des formes plus fondamentales du service de non-répudiation (avec preuve d'origine et preuve de remise). Par exemple, on peut mettre en œuvre la preuve de transport en affinant la transmission d'un message entre un expéditeur et un destinataire, de manière à obtenir une séquence d'échanges de messages, dont l'un est un acquittement de remise envoyé par un agent de transfert à l'expéditeur, puis en utilisant le service avec preuve d'origine pour protéger cet acquittement.

Annexe D

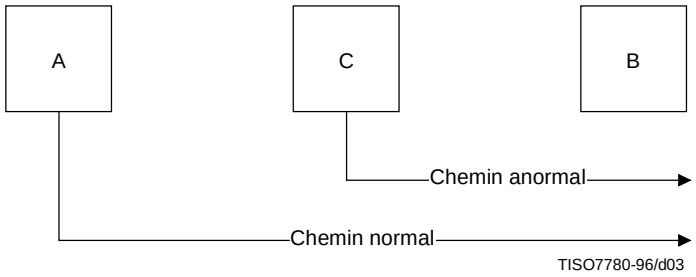
Reprise dans un service de non-répudiation

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

La reprise de sécurité se rapporte à des situations qui ne devraient pas se produire dans les circonstances normales. La réalité de la sécurité informatique est que des circonstances anormales se produisent cependant et qu'il vaut mieux s'y préparer.

En l'espèce, de nombreux mécanismes de non-répudiation se fondent sur des clés cryptographiques et sur le secret nécessaire pour protéger ces clés. La perte ou la divulgation d'une clé cryptographique doit être prévue par un plan de reprise pouvant être mis en œuvre immédiatement.

La situation suivante peut se produire lorsque des clés cryptographiques privées sont utilisées par un service de non-répudiation:



Les données signées par une partie fraudeuse (C), utilisant la clé privée négociée frauduleusement avec A, peuvent être transmises à une partie honnête (B). A un certain moment, on peut supposer que B aura des raisons d'interroger A, en lui présentant le message signé comme justificatif de l'action, à la suite d'une action (ou d'une omission d'action) concernant le message non autorisé. La partie A fera valoir qu'elle a perdu la clé privée correspondante et citera une déclaration publique en ce sens.

Si le litige est porté à l'attention d'un juge ou d'un arbitre, la responsabilité de A sera probablement déterminée par comparaison de la différence temporelle entre la déclaration publique de divulgation de clé et l'émission du message signé sans autorisation. Il est plus que probable que A sera tenu responsable si le message est antérieur à la déclaration de la divulgation de clé. Si la partie C a effectivement prédaté le message, A sera donc tenu responsable à moins que certaines mesures n'aient été prises pour régler autrement ce cas.

Afin de sortir d'une telle situation, il faut être en mesure de connaître le moment exact de la signature du message. Etant donné que le moment indiqué par C dans le message ne peut pas être considéré comme digne de foi, il est nécessaire d'invoquer un tiers de confiance qui enregistrera le message de l'une des manières suivantes:

- soit en copiant le message et sa signature dans un journal d'audit de sécurité approprié (c'est-à-dire en faisant appel à un notaire); et/ou
- en appliquant au message une contresignature comportant la date et l'heure de l'inscription, cet horodatage étant communiqué par un tiers de confiance indépendant (c'est-à-dire au moyen du service de pointage temporel).

En suivant cette procédure, une partie fraudeuse fournira malgré sa volonté la date et l'heure réelles de la signature. Un arbitre pourra alors rendre un jugement de responsabilité en faveur de la partie lésée (A) sur la base de ce qui suit:

en premier lieu, une comparaison entre la date/l'heure du message et la date/l'heure de la contresignature, qui doivent s'inscrire dans une fenêtre temporelle suffisamment étroite (par exemple 24 h);

en deuxième lieu, une comparaison entre la date/l'heure du message et la notification formelle de la perte ou de la divulgation de la clé.

De cette façon, l'emploi effectivement frauduleux d'une clé cryptographique perdue ou divulguée sera réduit à la fenêtre temporelle autorisée pour l'inscription des données par le service de pointage temporel.

La responsabilité de la partie A en cas de divulgation de clé dépend de la politique de sécurité en vigueur. Les brèches de sécurité ne sont pas toujours détectées immédiatement. Donc, même si la partie A avertit le tiers de confiance dès qu'elle prend connaissance de la divulgation, il reste possible à la partie C de créer des messages frauduleux après avoir forcé la clé privée de A et avant que A ait détecté cette divulgation.

Lors de la résolution des litiges, les deux instants suivants peuvent être applicables:

- l'instant auquel A a signalé la divulgation. La partie A répudiera tous les messages dont on pourra démontrer qu'ils ont été signés après cet instant. (La partie A devrait arrêter d'utiliser la clé privée dès qu'elle prend connaissance du fait que cette clé a été forcée);
- l'instant que A revendique comme étant antérieur à la divulgation de la clé. A ne répudiera pas les messages dont on pourra démontrer qu'ils ont été signés avant cet instant. Celui-ci peut ne pas exister, dans le cas où A a découvert la divulgation mais ne connaît pas avec certitude à quel moment la divulgation a eu lieu effectivement.

Annexe E

Interaction avec l'Annuaire

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

Une signature numérique peut être vérifiée au moyen d'une clé publique appropriée. Lorsque celle-ci est contenue dans un certificat d'utilisateur placé dans l'Annuaire, l'exactitude de la clé peut être vérifiée si l'on connaît la clé publique de l'autorité de certification.

Etant donné que l'autorité de certification qui a émis un certificat peut avoir changé sa clé publique depuis l'établissement du certificat, il est nécessaire d'avoir la possibilité de vérifier l'exactitude d'une clé publique «âgée». Comme la seule clé normalement connue est la clé publique qu'une autorité de certification possède actuellement, il faut qu'il y ait un lien entre la clé publique actuelle et les clés publiques âgées. Etant donné qu'un destinataire n'est pas conscient des modifications apportées à la clé d'une autorité de certification, il appartient aux différentes autorités de certification de permettre la vérification de leurs «anciens» certificats. Cette vérification peut s'effectuer de deux manières:

- en certifiant chaque clé publique âgée d'une autorité de certification en fonction de la clé publique actuelle de cette autorité;
- en certifiant chaque clé publique âgée d'une autorité de certification en fonction de la clé publique suivante de cette autorité.

Dans le premier cas, il est possible de vérifier directement la validité de l'ancienne clé publique de l'autorité de certification, qui correspond à la clé privée utilisée par cette autorité de certification pour émettre le certificat original.

Dans le deuxième cas, il faut pouvoir réunir une série de certificats et de vérifier progressivement la validité de l'ancienne clé publique de l'autorité de certification. Pour cela, on examinera d'abord le certificat dont la période de validité correspond à la date/l'heure du message signé puis on recherchera de façon récurrente un certificat dont la période de validité recouvre celle du précédent certificat mais est plus récente, afin de déterminer la valeur de la clé publique précédente de l'autorité de certification.

NOTE – En cas de possibilité de divulgation forcée d'une ancienne clé publique d'autorité de certification, la première méthode est préférable. Avec la seconde méthode en effet, la chaîne de certificats conduisant à la plus ancienne clé publique d'autorité de certification sera rompue et les plus anciennes clés publiques de l'autorité de certification deviendront automatiquement invalides.

Dans l'Annuaire, l'autorité de certification ne conserve pas la trace des certificats de liste de révocation des autres autorités de certification ou des utilisateurs de leurs certificats si ces derniers ne sont plus valides. Un utilisateur de preuve ou un tiers de confiance doit donc réunir toutes les informations nécessaires (c'est-à-dire y compris les listes de révocation, même si elles sont vides) pendant qu'elles sont encore disponibles, afin de prouver qu'une clé publique donnée a été valide à un certain moment.

Un certificat de liste de révocation contient la date à laquelle il a été émis par l'autorité. Il peut aussi contenir une autre date, qui peut aider à résoudre certains litiges: il s'agit de la date à laquelle l'utilisateur était encore certain que sa clé n'avait pas subi de divulgation forcée. Toutes les signatures émises par l'utilisateur avant cette date seront reconnues par celui-ci comme étant valides. Sans cette date, dans l'hypothèse du cas le moins favorable, toutes les signatures émises au cours de la période de validité du certificat de sécurité, seraient considérées comme invalides. Dans un environnement commercial, il est parfois très important pour un utilisateur qu'un document signé soit encore reconnu comme valide, même si la clé utilisée pour signer le message a été perdue. Bien que cette date soit facultative dans un certificat de liste de révocation, elle sera obligatoire si la clé du certificat correspondant est utilisée pour un service de non-répudiation.

Les relations de confiance peuvent évoluer dans le temps. Par exemple, un arbitre peut se fier à une autorité de certification à un moment, mais pas forcément à un autre. Le degré de confiance doit donc être signalé, de manière qu'un destinataire puisse savoir si un éventuel litige peut ou non être résolu à son avantage. Le type de relations de confiance qu'un arbitre donné reconnaît doit être exprimé. Ces conditions de confiance peuvent être modélisées au moyen des expressions suivantes, concernant la confiance:

- les autorités de certification totalement habilitées, dont on connaît la valeur de clé publique actuelle;
- les autorités de certification habilitées à émettre aussi bien des certificats d'autorité de certification que des certificats d'utilisateur;
- les autorités de certification uniquement habilitées à émettre des certificats d'utilisateur (mais non des certificats d'autorité de certification).

Ces informations doivent être mises gratuitement à la disposition de l'utilisateur de preuve. Elles peuvent prendre la forme d'un certificat de sécurité assorti d'une période de validité. Deux formes de certificats de politique de sécurité sont définies: les certificats de politique de sécurité dont la conservation est placée sous la responsabilité de l'arbitre et les certificats de politique de sécurité dont la conservation est placée sous la responsabilité du destinataire.

Annexe F

Bibliographie

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

– Recommandation UIT-T X.402 (1995) | ISO/CEI 10021-2:1996, *Technologies de l'information – Systèmes de messagerie: architecture globale*.

– Recommandation X.435 du CCITT (1991), *Systèmes de messagerie: système de messagerie avec échange de données informatisé*.

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

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Maintenance: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux pour données et communication entre systèmes ouverts**
Série Z	Langages de programmation