



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.842

(10/2000)

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Sécurité

**Technologies de l'information – Techniques de
sécurité – Lignes directrices pour l'utilisation et
la gestion des services de tiers de confiance**

Recommandation UIT-T X.842

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
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	
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 des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
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 et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

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

**RAPPORT TECHNIQUE ISO/CEI TR 14516
RECOMMANDATION UIT-T X.842**

**TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ –
LIGNES DIRECTRICES POUR L'UTILISATION ET LA GESTION DES SERVICES
DE TIERS DE CONFIANCE**

Résumé

La présente Recommandation | Rapport technique traite des services qui ont recours à des tiers de confiance (TTP). Elle propose des lignes directrices sur leur utilisation et sur la gestion des services, une définition claire des responsabilités et des services de base, la description et l'objet de ceux-ci, ainsi que les rôles et les responsabilités des TTP et des entités qui font appel à leurs services.

Elle distingue les différentes catégories de services TTP, notamment l'horodatage, la non-répudiation, la gestion de clés, la gestion de certificats et le notaire électronique.

Source

La Recommandation X.842 de l'UIT-T, élaborée par la Commission d'études 7 (1997-2000) de l'UIT-T, a été approuvée par l'AMN (Montréal, 27 septembre – 6 octobre 2000). Un texte identique est publié comme Norme Internationale ISO/CEI TR 14516.

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. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies 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.

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.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2002

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

TABLE DES MATIÈRES

	<i>Page</i>
1	Domaine d'application 1
2	Références normatives 1
2.1	Recommandations Normes internationales identiques 1
2.2	Paires Recommandations Normes internationales équivalentes par leur contenu technique 1
2.3	Autres références 1
3	Définitions 2
4	Aspects généraux 3
4.1	Base de l'assurance sécurité et de la confiance 3
4.2	Interaction entre le TTP et les entités utilisant ses services 4
4.2.1	Services TTP en ligne 4
4.2.2	Services TTP indirects 5
4.2.3	TTP indépendants 5
4.3	Interfonctionnement des services TTP 5
5	Aspects opérationnels et de gestion du TTP 6
5.1	Questions d'ordre juridique 6
5.2	Obligations contractuelles 7
5.3	Responsabilités 7
5.4	Politique de sécurité 7
5.4.1	Eléments de la politique de sécurité 8
5.4.2	Normes 9
5.4.3	Directives et procédures 9
5.4.4	Gestion du risque 9
5.4.5	Choix des protections 9
5.4.6	Implémentation de la sécurité dans les IT 10
5.4.7	Aspects opérationnels de la sécurité dans les IT 12
5.5	Qualité du service 13
5.6	Ethique 13
5.7	Taxes 13
6	Interfonctionnement 13
6.1	TTP-utilisateurs 13
6.2	Utilisateur-utilisateur 13
6.3	TTP-TTP 14
6.4	TTP-Service chargé de l'application des lois 14
7	Principales catégories de services TTP 15
7.1	Service d'horodage 15
7.1.1	Autorité d'horodatage 15
7.2	Services de non-répudiation 15
7.3	Services de gestion des clés 16
7.3.1	Service de production de clés 17
7.3.2	Service d'enregistrement de clés 17
7.3.3	Service de certification de clés 17
7.3.4	Service de distribution de clés 17
7.3.5	Service d'installation de clés 17
7.3.6	Service de stockage de clés 17
7.3.7	Service de dérivation de clés 18
7.3.8	Service d'archivage de clés 18
7.3.9	Service de révocation de clés 18
7.3.10	Service de destruction de clés 18
7.4	Service de gestion de certificats 18
7.4.1	Service de certificats de clé publique 18
7.4.2	Service des attributs de privilège 19

	<i>Page</i>
7.4.3 Service d'authentification en ligne fondé sur des certificats	20
7.4.4 Service de révocation de certificats	20
7.5 Services publics de notaire électronique	20
7.5.1 Service de production de preuves	21
7.5.2 Service de stockage de preuves	21
7.5.3 Service d'arbitrage	21
7.5.4 Autorité notariale	21
7.6 Service d'archivage numérique électronique	22
7.7 Autres services	23
7.7.1 Service d'annuaire	23
7.7.2 Service d'identification et d'authentification	24
7.7.3 Service de transposition en ligne	26
7.7.4 Services de récupération	26
7.7.5 Service de personnalisation	27
7.7.6 Service de contrôle d'accès	27
7.7.7 Service de signalisation des incidents et de gestion des alertes	27
Annexe A – Prescriptions de sécurité pour la gestion des TTP	29
Annexe B – Questions relatives à la gestion des autorités de certification	30
B.1 Exemple de procédure de processus d'enregistrement	30
B.2 Exemple de conditions à remplir par les autorités de certification	30
B.3 Politique de certification et déclaration relative aux méthodes de certification (CPS).....	32
Annexe C – Bibliographie.....	34

Introduction

Pour atteindre, en affaires, des niveaux de confiance suffisants dans l'utilisation des systèmes IT, il est indispensable de disposer des moyens techniques et légaux adéquats. Le monde commercial doit avoir la certitude que les systèmes IT offrent des avantages concrets et qu'il pourra tabler sur de tels systèmes pour l'aider à remplir ses obligations commerciales et à développer des perspectives d'affaires nouvelles.

L'échange d'informations entre deux entités sous-entend un élément de confiance; pour le destinataire, par exemple, l'identité de l'expéditeur et l'expéditeur lui-même se confondent et, inversement, l'expéditeur part du principe que l'identité du destinataire est en fait le destinataire auquel les informations sont adressées. Cet "élément de confiance implicite" n'est pas toujours suffisant, et il faut alors recourir à un "tiers de confiance" (TTP) pour assurer l'échange sûr des informations.

Les TTP ont notamment pour rôle de donner l'assurance que les messages et transactions de confiance, qu'ils soient de nature commerciale ou autre (communications officielles, par exemple), sont transmis au destinataire voulu et à l'emplacement visé, que ces messages sont reçus à temps, au moment opportun, et qu'en cas de litige commercial, des méthodes appropriées d'établissement et l'obtention de preuves permettent de déterminer ce qui s'est produit. Les services fournis par les TTP sont notamment ceux nécessaires à la gestion des clés, la gestion des certificats, l'identification et l'authentification, le service d'accès privilégié, la non-répudiation, les services d'horodatage, les services de notaire électronique ainsi que les services d'annuaire. Les TTP peuvent assurer ces services totalement ou en partie.

Un système TTP doit être conçu, mis en œuvre et exploité de manière à donner les assurances nécessaires au niveau des services de sécurité qu'il fournit et de satisfaire aux prescriptions réglementaires et légales qui s'appliquent. Les types et les niveaux de protection utilisés ou nécessaires varieront en fonction du type de service fourni et du contexte dans lequel se déroule l'application commerciale.

La présente Recommandation | Rapport technique a pour but:

- a) de donner des lignes directrices aux gestionnaires des TTP, aux concepteurs et au personnel d'exploitation afin de les aider dans l'utilisation et la gestion des TTP;
- b) de donner aux entités des lignes directrices relatives aux services assurés par les TTP et aux rôles respectifs et responsabilités des TTP et des entités qui font appel à leurs services.

La présente Recommandation | Rapport technique traite aussi des aspects additionnels suivants pour donner:

- a) un aperçu de la description des services fournis;
- b) la compréhension du rôle des TTP et de leurs caractéristiques fonctionnelles;
- c) la base de la reconnaissance réciproque des services fournis par des TTP différents;
- d) des lignes directrices sur l'interfonctionnement des entités et des TTP.

**RAPPORT TECHNIQUE
RECOMMANDATION UIT-T X.842**

**TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ –
LIGNES DIRECTRICES POUR L'UTILISATION ET LA GESTION DES SERVICES
DE TIERS DE CONFIANCE**

1 Domaine d'application

La fourniture et l'utilisation d'un service "tiers de confiance" (TTP) s'accompagnent d'un certain nombre de questions liées à la sécurité qui nécessitent une orientation générale ayant pour but d'apporter une assistance aux entités commerciales, concepteurs, fournisseurs de systèmes et services, etc. Il s'agit notamment de questions touchant au rôle et à la fonction du TTP, aux relations entre le TTP et les entités qui font appel à ses services, aux prescriptions de sécurité génériques, au type de sécurité que chacun est tenu d'assurer, aux solutions possibles en matière de sécurité et à la gestion de la sécurité du service TTP.

La présente Recommandation | Rapport technique propose des lignes directrices sur l'utilisation et la gestion de ces services, une définition claire des responsabilités et des services de base, la description et l'objet de ceux-ci, ainsi que les rôles et les responsabilités des TTP et des entités qui les utilisent. Il est destiné en premier lieu aux gestionnaires de systèmes, aux concepteurs, aux opérateurs de TTP et aux utilisateurs afin de les aider dans le choix des services TTP nécessaires en fonction des besoins, dans la gestion, l'utilisation et le déploiement opérationnel qui en résultent et dans l'établissement d'une politique de sécurité au sein du TTP. Il n'est pas destiné à être utilisé comme base d'évaluation formelle d'un TTP ou de comparaison formelle de TTP.

La présente Recommandation | Rapport technique distingue les principales catégories de services TTP, notamment l'horodatage, la non-répudiation, la gestion des clés, la gestion des certificats et le notaire électronique. Chacune de ces catégories est constituée de plusieurs services qui relèvent logiquement les uns des autres.

2 Références normatives

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.509 (2001) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion de systèmes ouverts – Cadres de sécurité pour les systèmes ouverts – Aperçu général.*
- Recommandation UIT-T X.813 (1996) | ISO/CEI 10181-4:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: non-répudiation.*

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.*

2.3 Autres références

- ISO/CEI 9798-1:1997, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 1: Généralités.*
- ISO/CEI 11770-1:1996, *Technologies de l'information – Techniques de sécurité – Partie 1: Cadre général.*
- ISO/CEI 11770-2:1996, *Technologies de l'information – Techniques de sécurité – Gestion de clés – Partie 2: Mécanismes utilisant des techniques symétriques.*
- ISO/CEI 11770-3:1999, *Technologies de l'information – Techniques de sécurité – Gestion de clés – Partie 3: Mécanismes utilisant des techniques asymétriques.*

- ISO/CEI TR 13335-1:1996, *Technologies de l'information – Lignes directrices pour la gestion de sécurité des technologies de l'information (TI): Partie 1: Concepts et modèles pour la sécurité des TI.*
- ISO/CEI TR 13335-2:1997, *Technologies de l'information – Lignes directrices pour le management de sécurité TI: Partie 2: Management et planning de sécurité TI.*
- ISO/CEI TR 13335-3:1998, *Technologies de l'information – Lignes directrices pour la gestion de sécurité TI – Partie 3: Techniques pour la gestion de sécurité TI.*
- ISO/CEI TR 13335-4:2000, *Technologies de l'information – Lignes directrices pour la gestion de sécurité TI – Partie 4: Sélection de sauvegardes.*
- ISO/CEI 13888-1:1997, *Technologies de l'information – Techniques de sécurité – Non-répudiation – Partie 1: Généralités.*
- ISO/CEI 13888-2:1998, *Technologies de l'information – Techniques de sécurité – Non-répudiation – Partie 2: Mécanismes utilisant des techniques symétriques.*
- ISO/CEI 13888-3:1997, *Technologies de l'information – Techniques de sécurité – Non-répudiation – Partie 3: Mécanismes utilisant des techniques asymétriques.*
- ISO/CEI WD 15443, *Technologies de l'information – Techniques de sécurité – Cadre pour l'assurance-sécurité TI.*

3 Définitions

NOTE – Dans l'ensemble de la présente Recommandation | Rapport technique, le terme "entité" peut désigner un être humain, une organisation, une composante matérielle ou un élément logiciel.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions données dans la Rec. CCITT X.800 et ISO 7498-2 s'appliquent: contrôle d'accès, imputabilité, audit, journal d'audit de sécurité, disponibilité, confidentialité, intégrité des données, transposition, signature numérique, chiffrement, authentification d'entité, intégrité, clé, gestion de clés, notarisation, non-répudiation, audit de sécurité, signature.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions données dans l'ISO 8402 s'appliquent: audit/évaluation.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions données dans la Rec. UIT-T X.509 | ISO/CEI 9594-8 s'appliquent: certificat d'attributs, certificat, autorité de certification (CA, *certification authority*).

Pour les besoins de la présente Recommandation | Rapport technique, les définitions données dans l'ISO/CEI 9798-1 s'appliquent: jeton.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions données dans l'ISO/CEI 9798-5 s'appliquent: autorité d'accréditation.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions suivantes données dans la Rec. UIT-T X.810 | ISO/CEI 10181-1 s'appliquent: clé privée, clé publique, scellé, clé secrète et tiers de confiance.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions suivantes données dans la Rec. UIT-T X.811 | ISO/CEI 10181-2 s'appliquent: certificat d'authentification et informations d'authentification (AI, *authentication information*).

Pour les besoins de la présente Recommandation | Rapport technique, les définitions suivantes données dans la Rec. UIT-T X.813 | ISO/CEI 10181-4 s'appliquent: générateur de preuve, notaire.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions suivantes données dans l'ISO/CEI 11770-1 s'appliquent: technique cryptographique asymétrique, technique cryptographique symétrique et horodatage.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions suivantes données dans l'ISO/CEI TR 13335-1 s'appliquent: actif, authenticité, impact, sécurité IT, politique de sécurité IT, fiabilité, risque résiduel, risque, analyse du risque, gestion du risque, protection, intégrité du système, menace et vulnérabilité.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions suivantes données dans l'ISO/CEI 13888-1 s'appliquent: non-répudiation d'approbation, non-répudiation de création, non-répudiation de remise, non-répudiation de connaissance, non-répudiation d'origine, non-répudiation de réception, non-répudiation d'envoi, non-répudiation de soumission, non-répudiation de transport.

Pour les besoins de la présente Recommandation | Rapport technique, les définitions supplémentaires suivantes s'appliquent:

3.1 autorité en charge des attributs (AA, *attribute authority*): entité bénéficiant de la confiance d'une ou de plusieurs entités pour l'établissement et la signature de certificats d'attribut. Il convient de noter qu'une autorité de certification peut également être une autorité en charge des attributs;

3.2 autorité d'enregistrement (RA, *registration authority*): entité responsable de l'identification et de l'authentification des sujets de certificats, qui n'est néanmoins ni une autorité de certification ni une autorité en charge des attributs, et par conséquent ne signe ni ne délivre de certificats. Une autorité d'enregistrement peut apporter son aide au cours des processus de demande de certificat ou de révocation ou des deux.

4 Aspects généraux

Un tiers de confiance (TTP, *trusted third party*) est une organisation ou son représentant qui offre un ou plusieurs services de sécurité et qui jouit de la confiance d'autres entités pour les activités liées à ces services.

Le TTP a pour fonction d'offrir des services à valeur ajoutée à des entités qui souhaitent rehausser les niveaux de confiance et de sécurité dans les services dont elles disposent et à permettre des communications sûres entre partenaires commerciaux. Les TTP doivent présenter des avantages au niveau de la confidentialité, de l'intégrité et de la disponibilité des services et des informations intervenant dans les communications liées aux activités commerciales. Les TTP doivent pouvoir interfonctionner les uns avec les autres et avec les entités.

Les entités doivent pouvoir choisir les TTP auxquels ils font appel pour obtenir les services recherchés. Inversement, les TTP doivent avoir la possibilité de choisir les entités auxquelles ils offriront leurs services.

Pour être efficace, le TTP doit généralement:

- a) fonctionner dans un cadre légal qui est le même pour toutes les entités participantes;
- b) offrir une gamme de services et des prestations minimales clairement définies;
- c) disposer de politiques bien définies, en particulier d'une politique de sécurité reconnue;
- d) être géré et exploité d'une manière sûre et fiable, au moyen d'un système de gestion de la sécurité des informations et de systèmes IT de confiance;
- e) se conformer aux normes nationales et internationales qui s'appliquent;
- f) se conformer à un code de conduite communément admis;
- g) publier des déclarations concernant les pratiques;
- h) enregistrer et archiver tout élément de preuve se rapportant à ses services;
- i) s'en remettre à un arbitrage indépendant sans compromettre la sécurité;
- j) fonctionner de manière indépendante et impartiale (conforme aux règles d'accréditation); et
- k) assumer des responsabilités dans les limites définies de disponibilité et de qualité du service.

4.1 Base de l'assurance sécurité et de la confiance

L'utilisation du TTP et de ses services dépend essentiellement de la constatation que d'autres TTP et entités auront confiance en ses services. Cette confiance résulte de la certitude que le TTP est géré correctement et que ses services fonctionnent de manière sûre. Il doit donc garantir que lui-même et les services qu'il fournit sont conformes aux politiques définies. La politique de sécurité en particulier doit porter sur tous les aspects de sécurité qui se rapportent à la gestion du TTP et au fonctionnement de ses services.

La confiance peut être établie au moyen de preuves relatives aux aspects de gestion et de fonctionnement. Il doit être prouvé que les aspects de gestion sont correctement et suffisamment pris en compte pour que les objectifs soient entièrement atteints, que le système de gestion soit efficace et adapté de manière à minimiser les risques et à faire face aux menaces, et que les mesures de protection soient bien documentées et bien comprises par le personnel, qu'elles ne soient pas périmées ou supplantées et qu'elles soient mises en œuvre correctement.

Afin d'accroître la confiance en ce qui concerne les aspects de gestion et de fonctionnement, le TTP doit en particulier fournir les preuves:

- a) qu'une politique de sécurité adéquate est en place;
- b) que les problèmes de sécurité ont été résolus au moyen d'une combinaison de procédures et de mécanismes de sécurité correctement mis en œuvre;

- c) que les activités se déroulent correctement et conformément à un ensemble clairement défini de rôles et de responsabilités;
- d) que les interfaces et procédures pour communiquer avec les entités sont adaptées aux fonctions qui ont lieu d'être assurées et qu'elles sont utilisées correctement;
- e) que les dispositions réglementaires sont respectées par la direction et le personnel et qu'elles cadrent avec un niveau de crédibilité fixé ou visé;
- f) que la qualité des procédés, des activités et des méthodes de travail a été effectivement approuvée;
- g) que le TTP satisfait à ses obligations contractuelles conformément à un contrat formel avec les utilisateurs;
- h) que les questions touchant à la responsabilité sont clairement comprises et acceptées;
- i) que la conformité aux lois et règlements est suivie et contrôlée;
- j) que les dangers connus et les moyens de les limiter sont clairement identifiés;
- k) qu'une évaluation des dangers et des risques est effectuée initialement pour être réexaminée/mise à jour régulièrement afin que les conditions de confidentialité, d'intégrité, de disponibilité et de fiabilité soient satisfaites;
- l) que les mesures appropriées au niveau de l'organisation et du personnel sont prises;
- m) que le TTP est fiable et que cette fiabilité peut être vérifiée et confirmée;
- n) que le TTP est surveillé par une certaine autorité administrative supervisant qu'il fonctionne conformément aux règles d'accréditation.

Les détails sont examinés à l'article 5 "Aspects opérationnels et de gestion du TTP".

Les divers types d'activité commerciale et d'application nécessiteront des niveaux différents de confiance et éventuellement de puissance des mécanismes et procédures de protection. A titre d'exemple, le niveau de confiance requis pour l'authentification d'une transaction administrative peut être différent de celui qui s'applique à une transaction financière, niveau qui à son tour peut être différent de celui exigé par certaines applications militaires. Les niveaux de confiance résultent des différences dans les politiques et les normes de sécurité et la manière dont elles sont mises en œuvre.

4.2 Interaction entre le TTP et les entités utilisant ses services

Du point de vue de la communication, le TTP et les entités communicantes peuvent adopter différentes configurations: directe, indirecte ou indépendante. Un exemple de chacune est donnée aux § 4.2.1 à 4.2.3.

Certains services de TTP peuvent présenter d'autres configurations, qui peuvent influencer les services que le TTP pourra assurer, par exemple l'opportunité de l'échange, le refus de prise en charge du service, l'enregistrement de la preuve, ainsi que les caractéristiques correspondantes telles que le délai de révocation d'un certificat.

4.2.1 Services TTP en ligne

Une disposition en ligne est nécessaire lorsque deux ou plusieurs entités appartiennent à des domaines de sécurité différents et qu'elles n'utilisent pas les mêmes mécanismes de sécurité. Dans ce cas, les entités n'ont pas la capacité d'effectuer des échanges directs et sûrs. Toutefois, le TTP placé directement sur le trajet de communication entre les entités peut contribuer à la sécurité des échanges comme indiqué à la Figure 1.

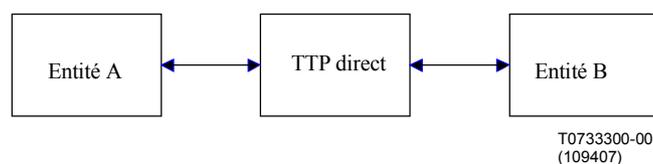


Figure 1 – Service TTP direct entre entités

Les services TTP directs peuvent porter sur les services d'authentification, de transposition et des attributs de privilège, et le TTP peut jouer un rôle au niveau de la non-répudiation, du contrôle d'accès, de la récupération des clés, de la confidentialité et de l'intégrité des données transmises.

4.2.2 Services TTP indirects

Lorsqu'une entité, ou les deux, demande au TTP indirect de fournir ou d'enregistrer des informations liées à la sécurité, le TTP intervient dans tous les échanges de sécurité initiaux. Son intervention n'est toutefois pas nécessaire dans les échanges suivants et il n'est pas placé sur le trajet de communication (Figure 2).

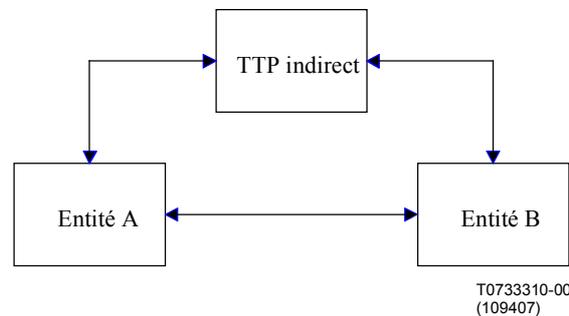


Figure 2 – Service TTP indirect entre entités

Les services TTP indirects peuvent porter sur l'authentification, la certification et les attributs de privilège, et le TTP peut jouer un rôle au niveau de la non-répudiation, du contrôle d'accès, de la gestion des clés, de la remise des messages, de l'horodatage, de la confidentialité et des services d'intégrité.

4.2.3 TTP indépendants

Un troisième type de configuration est celui du TTP indépendant. Dans ce cas, le TTP n'a pas d'interaction directe avec les entités pendant l'échange confidentiel, mais les données précédemment produites par le TTP sont utilisées par les entités comme le montre la Figure 3 (traits discontinus).

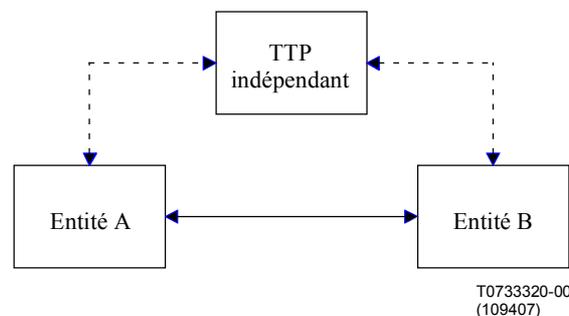


Figure 3 – Service TTP indépendant entre entités

Les services de TTP indépendant sont notamment l'authentification, la certification, l'attribut de privilèges, la non-répudiation, les services de répartition et de récupération des clés.

4.3 Interfonctionnement des services TTP

Un TTP peut offrir plusieurs services, qui sont décrits dans à l'article 7. L'ensemble des services peut être fourni par un seul TTP ou par plusieurs TTP. La fourniture des services peut aussi se faire en plusieurs endroits. Dans ce cas, les tâches et les devoirs doivent être définis et doivent figurer dans un contrat officiel, et il doit être tenu compte des incidences techniques et organisationnelles. Pour la gestion du TTP, on peut envisager des prescriptions supplémentaires en fonction de l'architecture de celui-ci (responsabilité et emplacement), en particulier en ce qui concerne la sécurité.

NOTE – Chaque service peut imposer que soient respectées des prescriptions particulières relatives à la sécurité. Si possible, il est généralement recommandé de séparer, parmi les aspects de gestion et opérationnels d'un TTP, les aspects généraux des aspects propres à chaque service. Un système de gestion structuré en modules est plus simple à manier lorsque des modifications se produisent, en particulier l'identification des incidences critiques en matière de sécurité lorsque ces modifications sont faites.

5 Aspects opérationnels et de gestion du TTP

A cet effet, il conviendrait de disposer d'une stratégie globale tenant compte des questions faisant l'objet des paragraphes ci-après. L'engagement du TTP à fournir des services se rapportant à la sécurité doit se présenter sous la forme d'une politique documentée, formelle. Il est recommandé que le TTP suive des directives concernant la protection de ses services. On trouvera des directives générales pour la gestion de la sécurité des services IT (GMITS) dans l'ISO/CEI TR 13335-1, 13335-2, 13335-3 et dans les Annexes A-H de 1335-4.

Selon les services fournis par le TTP, il est nécessaire de prendre de nombreuses décisions. Il faut non seulement définir les politiques qui régissent les services, mais également définir des politiques plus spécifiques, telles que celles qui portent sur l'apposition et la validation des signatures. Ces deux types de politiques auront des implications et des conséquences dont il doit être tenu compte à l'avance. En outre, les équipements techniques et non techniques dépendent les uns des autres, par exemple, la fourniture de services d'annuaire au moyen du protocole de statut des certificats en ligne ou de la liste d'annulation de certificats. Tous ces facteurs conduiront à des réalisations techniques et auront des conséquences dont il doit être tenu compte à l'avance. On trouvera un exemple de politique de sécurité traitant des certificats de clé publique dans "Internet X.509 Public Key Infrastructure, RFC 2527: Certificate Policy and Certification Practices Framework".

5.1 Questions d'ordre juridique

En plus de la précision de base des services particuliers qu'il offre, par exemple l'heure exacte pour une autorité d'horodatage, le TTP doit faire face à des responsabilités étendues pour répondre aux attentes de ses utilisateurs. Il s'agit de dispositions sans faille relatives à la confidentialité, l'intégrité, la disponibilité, le contrôle d'accès, la responsabilité, l'authenticité, la fiabilité, le secret, l'éthique (le droit d'utilisation, par exemple), compte tenu des aspects juridiques (lois et règlements), des techniques et mécanismes, et des aspects financiers. Tout manquement à ces responsabilités, accidentel ou conscient, peut entraîner des pertes substantielles pour l'utilisateur, et celui-ci cherchera réparation auprès du TTP. Afin de gérer les attentes des clients, d'une part, et de limiter les responsabilités, d'autre part, il convient d'établir entre le TTP et ses utilisateurs un contrat qui les lie officiellement. Un tel contrat devrait traiter au moins des aspects juridiques touchant aux questions suivantes:

- a) la responsabilité;
- b) le secret, surtout l'observation des lois sur la protection des données;
- c) les droits de copyright et de propriété intellectuelle;
- d) le recours à la cryptographie;
- e) l'interception et l'accès légaux;
- f) la légalité d'un service liant les parties, celui des signatures numériques, par exemple;
- g) le caractère anonyme des entités;
- h) le droit de vérifier, par exemple les titres;
- i) les conditions juridiques et réglementaires applicables à la juridiction et au secteur;
- j) les types de service à fournir;
- k) les dispositions relatives à l'accès, notamment les méthodes acceptées, les procédures d'acceptation d'un utilisateur (ou de changement d'utilisateur);
- l) les procédures de résolution des problèmes (y compris les points de contact autorisés);
- m) les responsabilités relatives aux besoins en matériel et en logiciel, en gestion et en contrôle des changements;
- n) les dispositions pour signaler, notifier et analyser les incidents touchant à la sécurité.

Les engagements et les responsabilités du TTP doivent cadrer sa capacité financière et les mandats ou garanties reçus d'autres entités. Les entités doivent prendre l'engagement que les informations qu'elles transmettent au TTP sont protégées contre la divulgation, sauf indication contraire figurant dans leur contrat. Le TTP doit satisfaire aux demandes légitimes de protection des informations personnelles, surtout celles qui se rapportent à la protection technique et organisationnelle appropriée des bases de données contenant des informations personnelles.

Le commerce électronique est international par nature et les TTP doivent satisfaire à toutes les obligations officielles découlant des lois, règlements et traités nationaux et internationaux. La conformité avec certaines de ces obligations peut avoir un effet significatif sur la conception et l'implémentation du TTP.

Les notions de responsabilité et le cadre légal de base peuvent être différents selon les pays. Pour cette raison, il conviendra d'adapter les lignes directrices générales de manière à répondre aux besoins des systèmes juridiques individuels. Lorsque la législation nationale relative aux TTP n'est pas la même de part et d'autres des frontières, les TTP qui souhaitent permettre à leurs utilisateurs de communiquer au-delà des frontières doivent disposer d'un accord contractuel spécial tenant compte des différences entre les deux juridictions.

Lorsque les communications traversent des frontières, les TTP concernés doivent être conscients des conséquences juridiques qui en résultent en ce qui concerne les différences ou incompatibilités éventuelles entre les politiques de sécurité et les énoncés de méthode respectifs.

5.2 Obligations contractuelles

Les contrats formels entre le TTP et les entités qui utilisent ses services doivent clairement énoncer les responsabilités du TTP, la qualité du service à fournir et les responsabilités des entités en question.

Le contrat doit préciser la politique de gestion et d'organisation du TTP ainsi que les procédures d'exécution. Le TTP doit également publier un énoncé des méthodes qui décrit ce que les entités sont en droit d'attendre des services du TTP afin de définir clairement et publiquement les contraintes et aspects opérationnels, la qualité du service, les questions d'éthique et la taxe à payer par l'abonné.

Le contrat doit spécifier clairement les dispositions décrivant la manière dont le TTP se conforme aux législations et règlements ainsi que les juridictions qui s'appliquent respectivement à l'exploitation et au règlement des différends.

Une erreur du TTP, accidentelle ou intentionnelle, peut entraîner des pertes substantielles au niveau des affaires. Pour que la confiance dans les services de TTP soit clairement établie, les limites de la responsabilité du TTP doivent être fixées dans le contrat avec les utilisateurs. Le cas échéant, la responsabilité doit être couverte par un contrat d'assurance applicable en cas de différend. Ce contrat entre le TTP et ses utilisateurs doit également préciser la couverture requise.

Le contrat doit contenir la liste de toutes les questions touchant aux responsabilités entre le TTP et ses utilisateurs afin que ces derniers puissent obtenir des conseils professionnels appropriés pour obtenir l'assistance juridique nécessaire sur toute question se rapportant à la fourniture et à l'utilisation des services du TTP.

Le contrat doit contenir la description des utilisations envisagées du service et les paramètres d'exploitation, et doit permettre au service d'être annulé si l'une des parties contractantes l'utilise de manière inappropriée ou illégale.

Le contrat doit contenir des dispositions indiquant clairement qu'il est possible de recourir à un arbitrage indépendant et impartial pour aider à résoudre les différends entre le TTP et ses utilisateurs.

Le contrat doit spécifier la mesure dans laquelle sera protégé le caractère privé des informations personnelles et autres informations sensibles, ainsi que les circonstances dans lesquelles leur divulgation peut avoir lieu.

5.3 Responsabilités

Le TTP doit définir dans quelle mesure sa responsabilité est engagée dans le fonctionnement sûr de son service. De plus, il doit cerner l'étendue des responsabilités pouvant être acceptées au niveau des atteintes à la sécurité.

Les responsabilités du TTP et celles de l'utilisateur doivent être clairement énoncées dans tout contrat formel qui est établi entre l'utilisateur et le TTP. La plupart des responsabilités doivent figurer dans le contrat, certaines étant définies seulement dans le cadre particulier de la transaction, d'autres étant les niveaux de qualité standard.

D'autres documents joints au contrat, par exemple ceux qui définissent les services à fournir, l'accord de service et toute annexe technique, déterminent également les responsabilités respectives des diverses entités concernées. Ces documents font partie de l'accord contractuel global.

5.4 Politique de sécurité

Lorsqu'il offre et fournit des services liés à la sécurité, le TTP s'impose certaines obligations au niveau de la confiance pouvant être accordée aux services en question ainsi qu'une politique de sécurité officielle, documentée, pour l'organisation offrant le service.

La politique de sécurité du TTP est un instrument de la plus haute importance permettant de décrire toutes les activités essentielles et importantes à mener pour instaurer la confiance en la gestion du TTP et en l'exploitation de ses services et l'accroître. Une politique de sécurité du TTP doit donc non seulement concerner des questions de sécurité spécifiques mais aussi aborder tous les aspects liés aux services du TTP. L'élaboration et la maintenance d'une politique de sécurité du TTP doivent se faire de manière systématique et logique.

Comme indiqué dans l'Annexe A de l'ISO/CEI TR 13335-3, la politique de sécurité du TTP doit être formée de deux parties:

- a) une politique de sécurité générale qui traite de manière concise les aspects non techniques relatifs à la sécurité et à la confiance dans les services TTP;
- b) une politique de sécurité à caractère technique qui traite d'une manière concise de tous les aspects techniques relatifs aux fonctions liées à la sécurité et à la confiance, avec la description des méthodes, des procédures, etc., qui se rapportent à ces aspects techniques.

Une évaluation rigoureuse de la sécurité des services TTP en vigueur permet de confirmer que les systèmes techniques répondent au niveau de confiance indiqué dans la politique de sécurité du TTP.

La politique de sécurité du TTP a une importance fondamentale dans le maintien de la confiance, d'une part entre les systèmes en ce sens qu'elle spécifie les bases des audits continu (interne) et périodique (interne et externe) de la sécurité, d'autre part dans les systèmes et dans l'organisation qui fournit le service.

L'engagement que prend le TTP d'assurer un service du domaine de la sécurité doit se présenter sous la forme d'une politique de sécurité formelle, dûment étayée. La politique de sécurité doit tenir compte de tous les objectifs, sujets et dangers possibles relatifs aux services fournis ainsi que les sécurités nécessaires pour éviter ou limiter les effets de ces dangers. Elle doit décrire les règles, les directives et les procédures relatives à la manière dont sont assurés les services spécifiés et la garantie de sécurité associée.

5.4.1 Éléments de la politique de sécurité

La teneur de la politique de sécurité du TTP dépendra des services fournis. La politique de sécurité doit former un cadre qui traite des questions de sécurité relatives à divers éléments. Les éléments techniques de la politique de sécurité du TTP constituent la base de toute évaluation technique liée à la sécurité. Comme indiqué dans l'ISO/CEI TR 13335-2, la politique de sécurité du TTP doit englober au moins les éléments suivants:

- a) les prescriptions de sécurité relatives aux technologies de l'information, par exemple en termes de confidentialité, d'intégrité, de disponibilité, d'authenticité et de fiabilité, surtout vis-à-vis de l'opinion des détenteurs d'informations;
- b) l'infrastructure organisationnelle et l'attribution des responsabilités;
- c) l'intégration de la sécurité dans le développement et la fourniture du système;
- d) l'information et la formation;
- e) les directives et les procédures;
- f) l'établissement de catégories pour le classement de l'information;
- g) les stratégies de gestion du risque;
- h) les plans d'intervention;
- i) les questions de personnel, une attention particulière étant accordée aux postes de confiance, au personnel de maintenance et aux administrateurs de systèmes, par exemple;
- j) les obligations légales et réglementaires;
- k) la gestion de la sous-traitance; et
- l) la manière de traiter les incidents.

L'implémentation de la politique de sécurité du TTP relative aux prescriptions techniques, administratives et organisationnelles de la sécurité doit surtout mettre l'accent sur les nécessités suivantes:

- a) l'assurance que le TTP exerce ses fonctions de telle manière que l'intégrité du système ne puisse pas être affaiblie ou mise en danger;
- b) l'intégrité des données de l'entité, qu'elles soient complètes, non modifiées et que leur source ou leur origine puisse être vérifiée;
- c) que les entités autorisées sont assurées de la disponibilité et de l'accès aux services et aux informations auxquels elles ont droit;
- d) le caractère confidentiel des informations sensibles et privées confiées par l'entité au TTP;
- e) les procédures de vérification de la sécurité des systèmes du TTP.

5.4.2 Normes

Le TTP doit se conformer aux normes qui s'appliquent. Celles-ci peuvent être des normes internationales, nationales, régionales, du secteur industriel, des normes ou règles des grandes sociétés, choisies et appliquées conformément aux prescriptions de sécurité de leurs organisations. Les avantages en sont l'interopérabilité, la sécurité intégrée, l'uniformité, la portabilité et l'interfonctionnement des organisations. Si plusieurs organisations différentes voient le jour et qu'elles utilisent leurs propres systèmes et produits sur la base de normes propriétaires, le risque existe de voir surgir à court terme des problèmes d'interopérabilité en raison des différences de méthodes. Les normes doivent être examinées à deux niveaux, les normes détaillées s'appliquant à des technologies spécifiques et leur utilisation, et les normes d'interopérabilité entre des technologies différentes.

5.4.3 Directives et procédures

Les directives et procédures sont des éléments nécessaires d'une politique de sécurité de TTP. Elles englobent les dispositions réglementaires nécessaires établies par l'organisation ainsi que les procédures d'orientation nécessaires à l'organisation pour fournir ces services à ses utilisateurs.

5.4.4 Gestion du risque

Pour atteindre un niveau acceptable de sécurité des systèmes IT, le TTP doit mettre en œuvre des méthodes de gestion du risque. Le processus de gestion du risque relatif à la sécurité d'un système IT du TTP doit être fondé sur une analyse détaillée du risque ou une méthode combinée. Il y a lieu d'évaluer toutes les informations pour déterminer la sensibilité des informations et les niveaux appropriés de protection pour maintenir la confidentialité, l'intégrité et la disponibilité. Les dangers, les risques et les systèmes de sécurité doivent être réévalués périodiquement. Les lignes directrices relatives au choix d'une stratégie appropriée de l'analyse des risques et une description détaillée du processus d'analyse du risque sont données dans l'ISO/CEI TR 13335-3. Sur la base des résultats de l'analyse du risque, il conviendra de choisir les systèmes de sécurité appropriés, de les tester et de les mettre en œuvre.

5.4.5 Choix des protections

Le TTP est exposé à de nombreux risques accidentels ou délibérés pouvant être d'origine humaine ou autre. Le TTP doit être protégé contre de tels risques au moyen de protections conçues pour diminuer sa vulnérabilité par la réduction des effets des incidents indésirables ou par l'amélioration de la facilité de rétablissement.

Les mesures, méthodes et procédures de sécurité doivent tenir compte de tous les aspects techniques, d'organisation, d'écriture, commerciaux, humains et légaux, et d'autre part être intégrées dans les dispositions, méthodes et procédures normales de l'organisation ou être coordonnées avec elles.

Les niveaux, coûts, mesures, méthodes et procédures de sécurité doivent être adéquats et proportionnels à la gravité des menaces, des effets possibles des dangers et du niveau de garantie accordé.

On trouvera des indications détaillées sur le choix des protections aux articles 8 à 11 de l'ISO/CEI TR 13335-4.

5.4.5.1 Mesures physiques et contextuelles

Il y a lieu de mettre en œuvre des mesures de sécurité physiques et environnementales visant à protéger les installations abritant les ressources du système, les ressources proprement dites ainsi que les installations nécessaires à leur fonctionnement. Le programme de sécurité physique et environnementale d'une organisation doit englober la commande d'accès physique, la protection contre le feu, les services d'appui correspondants (circuits électriques, plomberie et climatisation), la protection contre le vol, le câblage, etc.

Une organisation doit périodiquement vérifier la planification de la continuité commerciale qui traite de ces aspects pour veiller au maintien des fonctions commerciales et critiques dans l'éventualité de perturbations, importantes ou non, ou en cas de catastrophe. La planification de la continuité commerciale doit également porter sur les capacités de traitement des incidents qui donnent la capacité de réagir rapidement et efficacement aux discontinuités du fonctionnement normal (voir aussi le § 5.4.7.3, Plan d'intervention).

5.4.5.2 Mesures organisationnelles et personnelles

Une organisation doit avoir des politiques de sécurité qui contiennent les règles, directives et méthodes décrivant la manière dont les ressources sont gérées, protégées et réparties dans l'organisation. Toutes les fonctions importantes qui contribuent aux processus commerciaux doivent être identifiées et documentées, le personnel étant désigné et rendu responsable de ces fonctions.

Une organisation doit bénéficier de l'engagement à tous les niveaux de la gestion pour répondre aux attentes de la sécurité en matière de IT. Elle doit avoir la volonté de répondre aux exigences de la sécurité et d'attribuer les ressources nécessaires pour y parvenir.

Une organisation doit disposer de descriptions d'emploi définies au plan de la séparation des tâches et du moindre privilège, qui déterminent le niveau de difficulté de l'emploi sur la base des responsabilités et des niveaux d'accès, de l'examen de l'expérience professionnelle, de la formation et de la conscience professionnelle. L'attribution et la séparation judicieuses des responsabilités doivent avant tout permettre l'exécution des tâches, et cela d'une manière efficace.

Une organisation doit gérer efficacement ses accès informatiques afin de préserver la sécurité du système, y compris la gestion des comptes d'utilisateur, les vérifications et les modifications en temps opportun ou la suppression des accès.

5.4.5.3 Mesures propres aux IT

Un TTP qui fournit des services liés à la sécurité fait appel dans une large mesure aux systèmes IT. Des mesures de protection propres aux IT sont donc nécessaires pour les rendre sûrs et appropriés. Ces mesures de protection spécifiques peuvent être subdivisées en trois catégories, une catégorie technique, une catégorie concernant les communications et une catégorie liée à la mise en réseau. Les mesures de protection peuvent être choisies en fonction d'une évaluation détaillée, des préoccupations et des menaces en matière de sécurité ou du type de système IT.

- a) Les mesures en fonction des préoccupations et des menaces en matière de sécurité consistent en des protections de la confidentialité, de l'intégrité, de la disponibilité et de la responsabilité:
 - Confidentialité – La sécurité d'un service TTP peut être articulée autour d'une clé couramment utilisée (dans l'ensemble du système), un clé de validation par exemple. La protection de cette clé pourrait être assurée physiquement au moyen d'un matériel fiable et logiquement au moyen de codes communs.
 - Intégrité – Les informations confidentielles échangées à l'interface utilisateur-TTP pour les modes de communication en ligne, hors ligne et hors bande doivent être protégées contre toute modification, interruption ou blocage.
 - Disponibilité – Le TTP doit mettre en œuvre des mécanismes garantissant à ses utilisateurs l'accès aux services lorsqu'ils en ont besoin. Toute situation particulière d'indisponibilité, c'est-à-dire de refus du service, pourrait avoir une grande influence sur l'activité du TTP. Il convient d'envisager des mécanismes appropriés empêchant l'envahissement des télécommunications, les problèmes de routage et les interruptions de service.
 - Responsabilité – Il y a lieu de définir, pour le TTP et les utilisateurs de ses services, les responsabilités liées à chacune des activités. Le TTP doivent mettre en œuvre les mécanismes nécessaires pour permettre de retrouver l'entité responsable de tout événement ou action. Des journaux d'audit appropriés doivent être tenus afin de garder une trace de toutes les actions, transactions, processus, etc. La responsabilisation s'obtiendra par la surveillance du journal des vérifications de la sécurité et par des contrôles réguliers.
- b) Les mesures en fonction du type de système IT consistent en des protections du contrôle d'accès.
 - Contrôle d'accès – La protection contre l'utilisation illicite des services TTP peut être assurée au moyen de protections au niveau du contrôle d'accès, et il faut envisager l'implémentation de mécanismes appropriés dans les domaines suivants:
 - l'identification et l'authentification;
 - le contrôle d'accès physique;
 - le contrôle d'accès logique;
 - la cryptographie;
 - la gestion des privilèges.

On trouvera des précisions sur le contrôle d'accès dans l'ISO/CEI TR 13335-4 et dans la Rec. UIT-T X.812 | ISO/CEI 10181-3.

5.4.6 Implémentation de la sécurité dans les IT

5.4.6.1 Sensibilisation et formation professionnelle

La sensibilisation, l'information et la formation professionnelle de l'ensemble du personnel de l'organisation sont indispensables pour aboutir à une prise de conscience de la sécurité dans les systèmes d'information, de sa portée, de ses méthodes et de ses procédures. Sans l'accueil favorable et la participation du personnel à tous les niveaux, un programme de sensibilisation à la sécurité ne peut réussir. Il est impératif que la direction soit consciente du besoin de sécurité et de la nécessité de sensibiliser le personnel à cet effet. Un programme de sensibilisation doit donc convaincre le personnel que les systèmes IT sont exposés à des risques importants et que la perte d'informations, leur modification ou leur divulgation non autorisées peuvent avoir des conséquences majeures sur l'organisation et son personnel. On trouvera des précisions au sujet de la sensibilisation et la formation dans l'ISO/CEI TR 13335-2.

5.4.6.2 Fiabilité et garantie

La garantie de sécurité donnée par le TTP doit être le fruit:

- a) du choix des mécanismes appropriés pour les services fournis et la politique de sécurité;
- b) de l'implémentation correcte de ces mécanismes, surtout les aspects relatifs à la sécurité physique, l'environnement, la continuité commerciale, etc.;
- c) l'exploitation de ces mécanismes, qui dépend de la définition et du respect des procédures appropriées, surtout en ce qui concerne la gestion du personnel, le classement des informations, les autorisations, le traitement des incidents, etc.

Dans la fourniture de ses services, le TTP ne doit utiliser que des systèmes fiables. La fiabilité d'un système peut être prouvée par une évaluation formelle. On trouvera dans l'ISO/CEI 15408 (Critères communs) des précisions sur les critères d'évaluation qui aideront à décider quel est le niveau minimal de garantie que doit assurer le TTP.

Pour que le TTP soit fiable, il doit fonctionner conformément à ses spécifications. La certification est la procédure par laquelle un organisme indépendant donne l'assurance qu'un produit, une méthode ou un service est conforme aux prescriptions. Le processus de certification est constitué essentiellement d'une analyse des documents et d'une évaluation technique exécutée par une autorité de certification impartiale.

Une telle certification de conformité du TTP donne la garantie que la sécurité revendiquée est réellement présente. Les entités qui utilisent les services d'un TTP doivent utiliser de telles certifications comme base pour déterminer le niveau de confiance pouvant être accordé au TTP.

Selon les services TTP qu'il y a lieu de fournir, le processus de certification de conformité doit comporter l'analyse:

- a) de la conformité aux lois et règlements nationaux et internationaux régissant leurs statut, activités et niveaux de performance;
- b) de la conformité aux normes techniques;
- c) de la conformité à la politique de sécurité;
- d) de la conformité aux règles sectorielles ou professionnelles spécifiques; que celles-ci sont clairement définies, mises en œuvre et exécutées tant au sens administratif que technique;
- e) de la conformité aux codes de conduite les plus favorables;
- f) de l'adéquation des mesures de sécurité aux dangers, aux risques et à la politique de sécurité.

La décision que prend la direction d'une organisation d'obtenir une certification de conformité peut avoir des effets significatifs sur la conception et la réalisation projetées. Un exemple de prescription de sécurité s'appliquant aux TTP peut être trouvé dans le "German Digital Signature Act" et dans le règlement qui l'accompagne. Les autorités de certification des TTP peuvent elles-mêmes obtenir une certification de conformité. On trouvera au § B.2 un exemple des conditions à remplir à cet effet.

5.4.6.3 Accréditation des autorités de certification des TTP

On peut augmenter la confiance qui peut être placée dans un TTP par l'accréditation de l'autorité de certification conformément à un programme d'adéquation à l'application. Cette accréditation garantit que les procédures employées par les diverses autorités de certification sont analogues et que les résultats de leurs certifications sont comparables. L'accréditation est définie dans le Guide 2 de l'ISO/CEI. L'accréditation d'une autorité de certification signifie que celle-ci est communément reconnue compétente et fiable dans ses certifications de TTP; elle est donc un moyen additionnel de garantir la qualité des services fournis, ces organismes étant indépendants et exploités conformément à des règles communément admises.

Le responsable de l'accréditation évalue les aspects techniques et de procédure du système de gestion des autorités de certification conformément au Guide 61 de l'ISO/CEI ou à des systèmes analogues tels que les normes européennes de la série 450xx.

L'accréditation d'une autorité de certification est un moyen de garantir la qualité du travail de celle-ci, mais ne donne aucune indication sur les services offerts par un TTP donné. Chaque TTP définit lui-même ses services et l'autorité de certification TTP certifie la conformité de l'exécution.

5.4.7 Aspects opérationnels de la sécurité dans les IT

5.4.7.1 Audit/évaluation

Si l'évaluation est un moyen de prouver la fiabilité d'un système IT, l'audit et le diagnostic sont des moyens d'instaurer la confiance dans la politique de sécurité documentée et dans le système de gestion de la sécurité qui ont été élaborés. Une évaluation se fait dans le contexte des inspections de la sécurité des systèmes IT et sert de moyen d'évaluation suivant des critères établis à cet effet (on trouvera des précisions dans l'ISO/CEI 15408). L'audit s'utilise dans le contexte des bilans de gestion et dans les contrôles de base; c'est un moyen de vérifier que les éléments sont connus, documentés et exécutés. Le diagnostic s'utilise dans le contexte de l'amélioration du produit ou du processus, dont il évalue les forces et les faiblesses. Tous ces examens sont exécutés périodiquement ou sur demande.

L'audit sur la sécurité a pour objet de déterminer si les politiques de sécurité sont réellement mises en œuvre et permettent d'atteindre les objectifs souhaités. Un audit sur la sécurité est fondé sur l'examen des documents existants et sur l'inspection des mécanismes mis en œuvre et des contrôles de sécurité. Le TTP doit donc disposer d'une documentation mise à jour, appropriée et adaptée.

Les entités qui ont recours aux services des TTP peuvent demander que les inspections et audits soient effectués pour vérifier et valider le niveau de sécurité effectivement garanti. Elles peuvent demander que des audits soient effectués par leur propre équipe interne ou par des auditeurs externes indépendants. Les audits peuvent aussi être entrepris par le TTP dans le but d'évaluer lui-même la sécurité et les risques ou pour fournir aux clients une preuve de bon fonctionnement. Les autorités d'accréditation peuvent également demander des audits. Les audits peuvent être entrepris par suite d'un certain nombre de circonstances différentes, et cela périodiquement (annuellement, par exemple), sur demande, après une modification majeure ou après un incident. Un audit peut prendre en compte les aspects opérationnels du TTP tels que:

- a) la politique de sécurité;
- b) le choix des mécanismes de sécurité;
- c) l'implémentation des mécanismes de sécurité;
- d) l'organisation;
- e) les procédures;
- f) la gestion des changements;
- g) le personnel (aptitudes, formation, etc.);
- h) la sécurité physique;
- i) les aspects financiers;
- j) l'assurance responsabilité, quand elle s'applique;
- k) la documentation.

L'audit doit être exécuté conformément aux règles et pratiques professionnelles généralement applicables. Les auditeurs, qu'ils soient internes ou externes, doivent surtout veiller au respect strict des règles de confidentialité. Les organismes d'accréditation doivent donner les directives sur la manière de procéder. Le rapport d'audit qui sera rendu public ou remis aux entités utilisant les services du TTP doit être soigneusement vérifié car il ne doit contenir aucune information susceptible d'être utilisée pour amoindrir la sécurité du TTP.

NOTE – On trouvera une description et de plus amples détails sur l'audit de qualité et les procédures d'évaluation dans l'ISO 8402.

5.4.7.2 Traitement des incidents

Le TTP doit réagir à temps et de manière coordonnée afin de pouvoir faire face rapidement aux incidents et de limiter les effets des atteintes à la sécurité. Tout incident doit être signalé le plus rapidement possible après qu'il ait été détecté. Le TTP doit disposer de procédures permettant de faire face à des événements spécifiques en matière de sécurité qui sont détectés ou portés à son attention, par exemple la compromission d'une clé secrète ou d'une paire de clés publiques ou privées, ou encore la perte d'un jeton de sécurité personnel. Ces procédures doivent faire partie du plan d'analyse des incidents (IAS, *incident analysis scheme*) du TTP.

Il faut rendre difficile toute possibilité pour une entité de porter atteinte à la sécurité, fortuitement ou intentionnellement, et toute tentative de mauvaise utilisation des droits d'accès par une entité devrait, si possible, pouvoir être détectée par le TTP.

5.4.7.3 Plan d'intervention

La continuité des services du TTP doit être protégée contre les effets des défaillances ou des catastrophes, et il faut mettre en place un processus de gestion pour l'élaboration et le maintien des procédures relatives aux interventions. La planification des interventions doit traiter des points suivants:

- a) l'identification des fonctions commerciales majeures;
- b) l'identification des ressources internes et externes à l'appui de ces fonctions et services majeurs;
- c) le choix d'une stratégie de la continuité;
- d) l'établissement de plans et de procédures;
- e) la mise en œuvre de plans et procédures;
- f) l'essai et la mise à jour des plans et procédures.

On trouvera des indications détaillées sur la planification des interventions dans l'ISO/CEI TR 13335-3 et dans plusieurs normes nationales.

5.5 Qualité du service

Les prescriptions générales en matière de qualité du service sont la fiabilité, la disponibilité, la simplicité d'emploi, l'efficacité, l'implémentation correcte, la documentation et le contrôle d'accès.

5.6 Ethique

Les services du TTP doivent être fournis et utilisés de telle manière que les droits et intérêts légitimes de toutes les entités concernées soient respectés.

5.7 Taxes

Le TTP peut taxer l'abonné pour l'utilisation de ses services. Un décompte de toutes les taxes doit pouvoir être fourni sur la demande de l'entité utilisant les services, et les entités en questions doivent être informées des circonstances dans lesquelles les taxes peuvent être modifiées.

6 Interfonctionnement

L'interfonctionnement nécessite la connexion d'un certain nombre de TTP et d'entités sous la forme d'un réseau avec des interfaces, des protocoles et des formats de données clairement définis permettant à l'interfonctionnement d'avoir lieu. Chaque TTP fournit des services aux entités qui relèvent de son domaine, conformément à sa propre politique de sécurité. Il y a plusieurs sortes d'interfonctionnement, notamment: TTP-utilisateurs, utilisateur-utilisateur, TTP-TTP et, le cas échéant, TTP-service d'application de la loi.

Le TTP peut avoir des contrats de mandat avec d'autres TTP pour former un réseau, permettant ainsi à une entité d'un TTP de communiquer en toute sécurité avec des entités d'autres TTP. Lorsque le TTP ne peut fournir l'ensemble des services demandés, des contrats de mandat permettent à d'autres TTP de fonctionner en sous-traitance pour fournir ces services additionnels. Dans l'analyse des besoins d'interfonctionnement, il faut noter que la relation juridique entre le TTP et ses abonnés est différente de celle qui lie le TTP et des non-abonnés (par exemple des utilisateurs qui vérifient des signatures numériques sur la base de certificats de l'autorité de certification). On trouvera des exemples de structures d'interfonctionnement entre TTP (CA) dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

6.1 TTP-utilisateurs

Le moyen par lequel un utilisateur a une interaction avec le TTP pour demander et obtenir un service TTP est appelé l'interface d'utilisateur. Chaque utilisateur peut dialoguer avec le TTP de différentes manières selon le type de service proposé.

6.2 Utilisateur-utilisateur

Lorsque le TTP a accompli sa tâche, son assistance n'est plus requise pour la suite de la communication entre les entités. La relation entre les entités ainsi que la formalisation contractuelle de cette relation reposent dans une large mesure sur leur confiance dans le TTP et dans les mécanismes d'interfonctionnement des TTP.

6.3 TTP-TTP

L'interface TTP à TTP permet des communications sûres entre utilisateurs par l'échange d'informations relatives aux services de sécurité mis en œuvre. Dans beaucoup de domaines de la sécurité, on part du principe que les TTP se sont certifiés réciproquement. Par exemple, la Figure 4 ci-après représente les interfaces utilisées lorsque l'entité A demande au TTP A une clé secrète pour communiquer avec l'entité B (1); le TTP A transfère la clé secrète appropriée à l'entité A (3) et au TTP B (2), qui transfère la clé à l'entité B (3). Au moyen de cette clé commune, les entités A et B peuvent établir des communications sûres (4). Dans une variante, qui utilise la technique de la clé publique, l'entité A demande au TTP A (1) des communications sûres avec l'entité B. Le TTP A transfère le certificat de l'entité A au TTP B et demande le certificat de l'entité B au TTP B (2). Le TTP B transfère le certificat de l'entité A à l'entité B (3) et le certificat de l'entité B au TTP A (2), qui le transfère à l'entité A (3). Le certificat de l'entité B étant en possession de l'entité A, et réciproquement, il est possible d'établir des communications sûres entre les entités A et B (4).

De nombreux mécanismes différents peuvent être utilisés pour ces échanges au moyen de communications sûres.

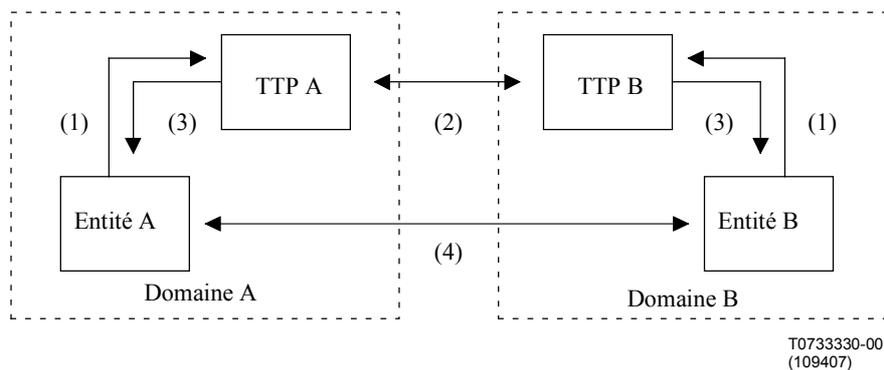


Figure 4 – Interfonctionnement de TTP dans des domaines différents

NOTE – Les mécanismes utilisés ne relèvent pas du domaine de la présente Recommandation | Rapport technique.

Il faut considérer qu'un service de sécurité donné peut résulter de la combinaison de TTP différents proposant des services complémentaires ayant éventuellement des niveaux de sécurité différents. Pour cette raison, il convient d'établir des règles relatives à l'évaluation du niveau de sécurité offert par les TTP et de proposer des méthodes relatives à l'évaluation du niveau de sécurité d'un service à plusieurs TTP.

L'examen qui suit s'applique dans les cas où le TTP est un autorité de certification (CA).

Les CA peuvent être organisées suivant des architectures hiérarchiques ou non hiérarchiques.

Dans une architecture hiérarchique, les trajets de certification suivent une hiérarchie allant de la CA racine à sa CA subordonnée en suivant l'architecture hiérarchique.

Dans une architecture non hiérarchique, les CA doivent se certifier réciproquement pour permettre l'emploi et l'échange en souplesse des certificats. Cette certification réciproque doit avoir lieu avec des niveaux de garantie élevés et suivant un code de conduite élaboré. Dès que la certification réciproque a été rétablie entre des CA, il est possible de construire les trajets de validation et les certificats de clé publique. Une entité ne doit avoir confiance que dans la clé de vérification d'une seule CA. Cette confiance s'étend alors via le trajet de certification à la clé publique de l'autre entité émise par l'autre CA.

6.4 TTP-Service chargé de l'application des lois

Le premier souci déclaré des services chargés de l'application des lois et des services de sécurité nationaux est que l'emploi à grande échelle des communications cryptées diminue la capacité de combattre le crime ou de prévenir les activités criminelles ou terroristes.

Cette interface, lorsqu'elle s'applique, dans les pays et dans ce type d'interaction, est le moyen par lequel le service chargé de l'application des lois peut demander et recevoir du TTP des informations archivées confidentielles. Ces informations permettront de déchiffrer des communications cryptées qui ont été légalement interceptées.

7 Principales catégories de services TTP

7.1 Service d'horodatage

Un service d'horodatage scelle un document numérique en y rattachant cryptographiquement une indication de temps sûre (généralement à une représentation hachée de celle-ci appelée sommaire de message ou empreinte de message) pour lui conférer un moyen de détecter toute modification telle qu'un antidatage et d'éviter les attaques par répétition et les autres contrefaçons.

Le service d'horodatage est fondé sur l'authenticité de l'horloge utilisée; pour cette raison, le TTP doit disposer d'un service d'horodatage utilisant une horloge à très hautes caractéristiques de fiabilité, de disponibilité et de confiance.

On peut créer un recueil de messages au moyen des techniques décrites dans l'ISO/CEI 10118-1, 10118-2, et 10118-3. Les jetons d'horodatage sont décrits dans l'ISO/CEI 13888-1.

Facultativement, le TTP qui fournit les services d'horodatage doit enregistrer tous les sceaux électroniques par ordre chronologique dans une archive permanente. Par ailleurs, on peut établir un service de vérification des horodateurs.

7.1.1 Autorité d'horodatage

Une autorité d'horodatage (TSA, *time stamp authority*) est un TTP qui crée des jetons horodateurs pour indiquer qu'un message existait à un instant donné.

La TSA fournit une "preuve d'existence" de ce message à un instant donné. On peut également y recourir lorsqu'il faut une référence temporelle fiable et que l'horloge disponible localement ne peut avoir la confiance de toutes les entités. La TSA a pour rôle d'horodater le cachet d'un message pour établir une preuve indiquant l'heure avant laquelle le message a été établi. L'horodatage peut ensuite être utilisé:

- a) pour vérifier qu'une signature numérique a été apposée avant l'annulation du certificat, permettant ainsi à un certificat de clé publique annulé d'être utilisé pour vérifier des signatures créées avant l'heure d'annulation;
- b) pour indiquer l'heure de soumission lorsqu'il est nécessaire de respecter impérativement une échéance;
- c) pour indiquer l'heure de la transaction.

La TSA:

- a) ne doit garantir que l'horloge fiable;
- b) doit introduire dans son jeton horodateur (l'heure choisie peut être l'heure GMT ou l'heure locale) une valeur augmentant de façon monotone représentant l'heure;
- c) doit produire un jeton horodateur à la réception d'une demande valable émanant du demandeur;
- d) doit introduire dans chaque jeton horodateur un identificateur désignant de manière unique la politique de confiance et de validation appliquée à la création du jeton;
- e) doit horodater uniquement une représentation hachée du message;
- f) doit signer chaque jeton horodateur au moyen d'une clé produite exclusivement à cet effet et indiquer dans le certificat correspondant cette propriété de la clé (des méthodes cryptographiques autres que la signature peuvent également être utilisées);
- g) doit inclure des informations de temps supplémentaires (par exemple les résultats sportifs ou de la loterie) dans le jeton horodateur si le demandeur le souhaite;
- h) conformément à la politique en vigueur, doit fournir au demandeur, en cas de nécessité, un reçu signé ou vérifié d'une autre manière comme étant sûr sous la forme d'un jeton horodateur adéquatement défini.

On trouvera des informations détaillées et un exemple de protocole d'horodatage dans le Document PKIX, Partie V, et dans l'ISO/CEI WD 18014.

7.2 Services de non-répudiation

Selon les mécanismes utilisés et la politique de non-répudiation en vigueur, le TTP peut participer à la fourniture de services de non-répudiation. La non-répudiation a pour objet, en vertu de l'ISO/CEI 13888-1, 13888-2 et 13888-3, de fournir une preuve vérifiable, sous la forme de données enregistrées reposant sur des valeurs de contrôle cryptographiques produites au moyen de techniques symétriques ou asymétriques, de l'approbation, de l'envoi, de l'origine, de la présentation, du transport, de la réception, de l'information et de la remise. Une composante importante de la non-répudiation, qui permet de donner la preuve vérifiable, est l'horodatage.

On peut utiliser deux méthodes de base pour décider si le TTP doit impérativement faire partie du service de non-répudiation.

- 1) En vertu de l'ISO/CEI 13888-2, il faut pour les services de non-répudiation reposant sur des techniques symétriques:
 - a) un service en ligne pour l'établissement de la preuve, sa vérification et la production d'enveloppes sûres;
 - b) un service hors ligne pour la personnalisation des clés appropriées dans un dispositif cryptographique de confiance, par exemple une carte à puce ou un module de sécurité.

Il est important de noter que la non-répudiation basée sur des techniques symétriques repose sur une seule clé, qui peut être utilisée par un TTP pour offrir des services de notaire. L'emploi de cette clé est restreinte et sa distribution aux entités doit être maintenue sous contrôle.

- 2) En vertu de l'ISO/CEI 13888-3, on peut spécifier des techniques asymétriques pour établir des mécanismes destinés à des services de non-répudiation de l'origine, de la remise, de la présentation et du transport.

Si un TTP n'intervient pas directement dans un service de non-répudiation on peut utiliser, pour établir l'infrastructure nécessaire, d'autres services de TTP tels que l'assignation de clé certifiée, avec ou sans production de clé, ou les services de gestion des certificats.

La Figure 5 représente un exemple de TTP fournissant des services de non-répudiation pour des entités A et B.

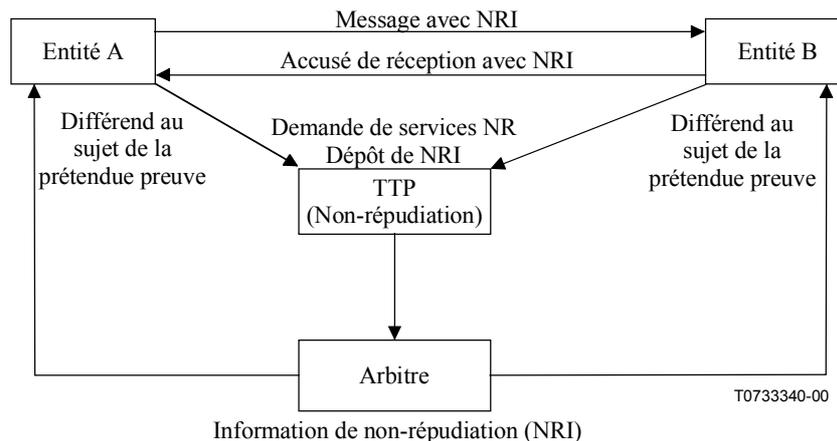


Figure 5 – Exemple d'architecture de non-répudiation

On trouvera d'autres précisions sur la participation du TTP à la fourniture de services de non-répudiation dans l'ISO/CEI 13888-1.

7.3 Services de gestion des clés

En vertu de l'ISO/CEI 11770-1, la gestion des clés s'appuie sur les services de base que sont la production, l'enregistrement, la certification, la distribution, l'installation, le stockage, la dérivation, l'archivage, la révocation, la désinscription et la destruction. D'autres services liés à la sécurité pouvant être utilisés sont notamment le contrôle d'accès, l'audit, l'authentification, les services cryptographiques et d'horodatage.

Un TTP en ligne peut faire fonction de serveur de gestion des clés à l'appui des services utilisant des techniques cryptographiques. Selon la composition des clés, le service peut être un service de répartition de clés (lorsque celles-ci sont produites par le TTP) ou un service de transposition des clés (lorsqu'elles sont produites par des entités et transmises à d'autres via le TTP).

7.3.1 Service de production de clés

Ce service est sollicité pour produire des clés d'une manière sûre pour un algorithme cryptographique donné. L'établissement de nombres secrets, imprévisibles, ayant des propriétés données, est décisive dans la production de clés. On peut, par exemple, établir des nombres aléatoires au moyen d'un générateur de nombres pseudo-aléatoires cryptographiquement sûr ou par une source aléatoire telle qu'une décroissance radioactive. Les divers éléments d'un nombre aléatoire sont la production de ce nombre aléatoire et sa validation, la production des paramètres du domaine et leur validation, la production de paires de clés et la validation de la clé publique. Une introduction utile aux nombres aléatoires, y compris la méthode de production, est donnée dans le Document RFC 1750.

Il importe d'envisager les éléments suivants, tant pour les techniques symétriques qu'asymétriques:

- a) des clés éventuellement modérées pour l'algorithme;
- b) l'utilisation de l'espace de clé complet.

7.3.2 Service d'enregistrement de clés

Dans ce cas le TTP est une autorité d'enregistrement accréditée chargée d'enregistrer les clés des entités, chaque clé enregistrée étant associée à une entité spécifique. Ce service englobe la tenue sûre et avisée d'un registre et des informations correspondantes, par exemple un registre des clés publiques d'une entité. Les clés publiques doivent être certifiées par une ou plusieurs autorités de certification. Pour augmenter la disponibilité et la fiabilité de ce service, les clés certifiées doivent être réparties dans de nombreux annuaires accessibles au public et fiables; une mise à jour périodique de tous les annuaires est nécessaire pour les besoins de concordance. Les services fournis par une autorité d'enregistrement de clés sont l'inscription et la désinscription. On trouvera des précisions sur le contenu d'un registre de clés dans l'Annexe B de l'ISO/CEI 11770-1.

7.3.3 Service de certification de clés

Dans ce cas le TTP est une autorité de certification accréditée qui crée des certificats de clé. L'autorité de certification horodate et signe les clés publiques ou les attributs pour les rendre valables et authentiques dans une infrastructure à clé de confiance. Les entités qui utilisent les certificats doivent faire confiance à la même autorité de certification ou au moins à une autorité commune dans une hiérarchie de certification. Les clés de certification peuvent être produites soit par un service de production du TTP, soit par le détenteur de la clé. Le service englobe également la recertification en cas d'expiration. Les certificats de clés publiques sont examinés en détail dans l'Annexe D de l'ISO/CEI 11770-1.

Il est important de noter que les services consistent:

- 1) à fournir la preuve de la détention de la clé privée par le détenteur qui s'en réclame;
- 2) à fournir la garantie de validité de la valeur de la clé publique proposée (et la validité d'un ensemble de paramètres de domaine en cas de nécessité),

peut être demandé parallèlement au service de certification ou dans le cadre de celui-ci.

7.3.4 Service de distribution de clés

Un service de distribution de clé a pour objet de distribuer les clés en toute sécurité aux entités autorisées. Selon la politique de sécurité du TTP, les clés doivent éventuellement être envoyées à d'autres services TTP, par exemple un service d'annuaire. Ces services peuvent être fournis par le même TTP ou par un autre. La répartition des clés entre les TTP ou entre les TTP et les entités, surtout lorsqu'elles sont distribuées par des voies peu sûres, doit être protégée au moyen de protocoles et de mécanismes cryptographiques. On trouvera des précisions sur les différents mécanismes de répartition des clés entre les entités dans l'ISO/CEI 11770-2 et des précisions relatives aux différents mécanismes pour agréer les clés secrètes et aux mécanismes de transport des clés secrètes et publiques dans l'ISO/CEI 11770-3. Des précisions sur les différents mécanismes qui ne sont pas décrits dans l'ISO/CEI 11770-3 sont données dans l'ISO/CEI 15946-3.

En vertu de l'ISO/CEI 11770-1, une occurrence particulière de répartition des clés est la transposition des clés. Le rôle d'un service de transposition des clés est de transposer des clés pour leur répartition entre les entités, c'est-à-dire que chaque entité partage une clé unique avec un centre de transposition de clés.

7.3.5 Service d'installation de clés

Ce service est indispensable avant qu'une clé puisse être utilisée étant donné qu'il la place dans un système de gestion de clés qui la protège de toute compromission.

7.3.6 Service de stockage de clés

Ce service assure le stockage de clés fréquemment utilisées ou de clés servant peu de temps, ou encore de clés de réserve, généralement dans un lieu physiquement séparé pour garantir la confidentialité et l'intégrité. Il est indispensable que toute tentative de compromission puisse être détectée.

7.3.7 Service de dérivation de clés

Ce service crée un nombre potentiellement important de clés au moyen d'une clé originale secrète appelée clé de dérivation, de données variables non secrètes et d'un processus de transformation. Cette clé de dérivation doit être spécialement protégée et il faut que le processus de transformation soit non réversible et non prévisible afin que la compromission d'une clé dérivée ne divulgue pas la clé de dérivation ou toute autre. Un nombre potentiellement important de clés sont créées par le processus de transformation au moyen d'une clé originale, appelée clé de dérivation, et de données variables non secrètes.

7.3.8 Service d'archivage de clés

Ce service est analogue au service de stockage de clés, mais il s'agit de conserver pour une longue durée des clés qui ne sont plus utilisées et qui pourraient être utiles beaucoup plus tard pour apporter des preuves dans le cas de certaines réclamations.

7.3.9 Service de révocation de clés

Ce service a pour but de désactiver une clé de manière sûre lorsque celle-ci est compromise ou suspectée de l'être. Il y a lieu de distribuer régulièrement la liste des clés révoquées. La révocation peut être demandée par le détenteur de la clé, par une autre personne autorisée ou par une entité de confiance s'il y a la moindre suspicion que la clé a été compromise. En vertu de l'Annexe D de l'ISO/CEI 11770-1, chaque entrée de la liste doit indiquer l'heure de révocation, l'heure de la demande et l'heure à laquelle la clé est devenue compromise ou suspectée de l'être. Dans certains cas, la révocation doit répondre à des restrictions temporelles précises, et il ne faut qu'un intervalle très réduit entre l'heure de la demande et la distribution de l'annonce de la révocation. Un TTP ne peut révoquer que les clés de ses clients, généralement en précisant à chacun d'eux quelles sont ces clés.

7.3.10 Service de destruction de clés

Dans ce cas, le TTP est une autorité d'enregistrement chargée de détruire les clés qui ne sont plus utilisées. Le TTP doit tout d'abord effectuer une désinscription pour supprimer l'association entre la clé et son entité. Cette opération est suivie de la destruction de la clé par l'élimination de toutes les informations qui s'y rapportent afin qu'elle ne soit plus récupérable. Cela inclut la destruction de toutes les copies des clés archivées, après un examen permettant de s'assurer qu'aucun élément archivé et protégé par ces clés ne sera plus jamais sollicité.

7.4 Service de gestion de certificats

Le format d'un certificat de clé publique et d'un certificat d'attribut est défini dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Le format du certificat d'attribut est compatible avec le certificat de la Rec. X.509 et n'est pas limité à un domaine d'utilisation précis. Cela est important puisqu'il est possible d'adresser le même "sujet" (par exemple une entité) avec les attributs (par exemple le nom d'entité) utilisés dans le certificat (clé publique) X.509. D'autres précisions relatives à la gestion des certificats figurent dans l'Annexe D de l'ISO/CEI 11770-1.

Les paragraphes ci-après traitent de certains services de gestion des certificats.

7.4.1 Service de certificats de clé publique

Une autorité de certification (CA) est un TTP qui établit des certificats de clé publique et prend soin des informations nécessaires pour la révocation des certificats ainsi émis. Il le fait en vérifiant l'identité du demandeur avant d'émettre un certificat de clé publique, qui porte sur une période de validité limitée. La CA devra s'assurer que le demandeur connaît la clé publique et que la clé publique du demandeur passe un test de validation et, si nécessaire, des tests de validation des paramètres du domaine.

La durée de vie des certificats de clé publique est gérée par le TTP fournissant les services de CA. La CA a la confiance de ses utilisateurs, qui est basée sur l'utilisation de mécanismes et d'équipements cryptographiques appropriés et sur la gestion professionnelle des méthodes de contrôle. Cette confiance est confirmée par une fonction d'audit indépendante qui rend les résultats de l'audit disponibles pour les entités. Les responsabilités de la CA sont notamment:

- a) identifier les entités dont les informations de clé publique sont présentées pour certification; des procédures pour décrire cet aspect sont décrites en détail au paragraphe B.1, des "Exemples de procédure de processus d'enregistrement";
- b) s'assurer de la qualité de la paire de clés asymétriques utilisée pour produire des certificats de clé publique;

- c) garantir le processus de certification et la clé privée utilisée pour signer les informations de clé publique;
- d) gérer les données spécifiques au système qui doivent être incluses dans les informations de clé publique telles que le numéro de série du certificat, l'identification de l'autorité de certification, etc.;
- e) attribuer et vérifier les périodes de validité;
- f) informer l'entité identifiée dans l'information de la clé publique que le certificat de clé publique a été émis; les moyens utilisés pour acheminer cette information doivent être indépendants de la méthode utilisée pour acheminer l'information de clé publique à la CA;
- g) veiller à ce que toutes les informations figurant dans un certificat soient conformes aux prescriptions de la politique applicable en matière de certificat, par exemple en s'assurant que deux entités différentes n'ont pas reçu la même identité et qu'elles peuvent donc être clairement distinguées;
- h) tenir à jour une liste des révocations et la publier;
- i) consigner toutes les étapes du processus de production d'un certificat de clé publique.

Une CA peut certifier l'information de clé publique d'une autre CA pour établir un certificat de clé publique. Dans ce cas, l'authentification peut faire intervenir une suite de certificats de clé publique. Le premier d'une telle série peut être obtenu et authentifié par des moyens autres que ceux utilisés pour les certificats de clé publique.

NOTE – Etant donné que le destinataire d'une signature numérique n'a pas nécessairement eu de contact antérieur avec la CA qui émet le certificat accompagnant la signature numérique, il faut un mécanisme par lequel le destinataire peut établir un niveau de confiance dans la CA. Cette confiance est établie par un processus de certification réciproque, un accord bilatéral entre les deux CA par lequel chacune peut émettre un certificat pour l'autre.

Plusieurs questions sont prises en compte dans la certification réciproque, notamment:

- a) les processus d'identification;
- b) la production de clés et les processus de stockage;
- c) la responsabilité;
- d) les processus de révocation;
- e) les processus de sécurité; et
- f) les différences dans les énoncés des politiques et méthodes.

7.4.2 Service des attributs de privilège

Quelques attributs de privilège peuvent changer plus fréquemment que d'autres attributs. Pour cette raison, on prévoit que seuls les attributs qui sont fréquemment utilisés et qui sont rarement modifiés devraient figurer dans un certificat de clé publique. Aussi convient-il d'utiliser une structure de données séparée (telle que des certificats d'attribut, des tickets, etc.) pour "garantir" ceux des attributs qui changent souvent (par exemple des limites de crédit, des privilèges d'accès, une capacité de représentation accordée par une entreprise, etc.).

Deux méthodes de base permettent de "protéger" les attributs:

- 1) les tickets – un ticket est une structure de données contenant plusieurs attributs cryptés par un TTP. De tels tickets sont utilisés par exemple dans Kerberos (RFC 1510) et peuvent contenir une identité d'entité, une adresse de réseau, etc.; et
- 2) les certificats d'attribut – un certificat d'attribut peut ou ne peut pas exister en combinaison avec un certificat de clé publique. La combinaison est possible étant donné que la clé publique associée au certificat de clé publique peut être utilisée pour prouver qu'une entité est le sujet réel du certificat d'attribut.

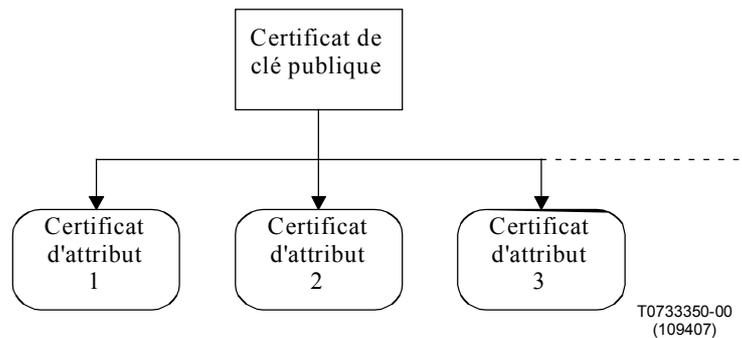


Figure 6 – Liens entre un certificat d'attribut et un certificat de clé publique

La Figure 6 illustre la deuxième approche, dans laquelle un certificat d'attribut se réfère sans équivoque à un certificat de clé publique. On peut établir un lien entre plusieurs certificats d'attribut et un certificat de clé publique. Des certificats d'attribut différents peuvent prendre en charge divers domaines d'utilisation, par exemple les questions liées au personnel (limite de crédit pour le commerce électronique) ou à l'autorité au sein d'une organisation.

Lorsqu'il n'attribue que des certificats d'attribut, le TTP agit comme autorité en charge des attributions (AA). Dans ce cas, les liens fonctionnels entre les certificats de clé publique et les certificats d'attribut, tels qu'ils sont décrits à la Figure 6, sous-entendent des accords appropriés entre la CA et la AA.

7.4.3 Service d'authentification en ligne fondé sur des certificats

Un TTP d'authentification en ligne se comporte comme un service de certification de certificats d'authentification; la récupération des certificats d'authentification est possible à l'échange d'authentification suivant. Un tel TTP est généralement appelé un serveur d'authentification.

7.4.4 Service de révocation de certificats

Une entité autorisée à révoquer des certificats qui souhaite révoquer le sien doit prendre contact avec la CA qui a accordé ce certificat pour l'aviser que ce certificat n'est plus valable. Lorsque la CA a vérifié l'état du certificat, elle produit une liste CRL en utilisant la signature de sa clé privée.

Une CRL est une liste signée numériquement qui contient les informations relatives aux certificats révoqués produits par la CA qui avait émis ces certificats.

Chaque CA doit gérer la CRL qui contient tous les certificats révoqués, et l'information CRL doit contenir un numéro de série unique et la date de révocation de ce certificat.

Une autre méthode consiste à utiliser un TTP en ligne comme serveur de validation de certificat donnant les informations tirées de l'état (y compris la révocation) d'un certificat donné.

7.5 Services publics de notaire électronique

Les services publics de notaire sont des services de haut niveau utilisant un certain nombre de services de base tels que l'horodatage, la certification, le service d'annuaire, l'archivage numérique et la non-répudiation. En principe un document sera remis au TTP, qui atteste ou certifie ce document au moyen de signatures numériques ou d'un autre moyen. Une partie du service peut être un service d'annuaire dans lequel on peut retrouver, dans une base de données ou un répertoire, des informations telles que des documents précédemment certifiés.

Un service public de notaire peut attester et certifier certaines catégories de documents, par exemple qu'un document a existé à un instant donné afin de lui conférer crédibilité et authenticité. Un tel service peut être utilisé en cas de médiation ou de différend entre des entités et peut être autorisé par une autorité.

Le service de notarisation fonctionne comme un notaire public électronique. Il a la capacité d'enregistrer des documents horodatés portant une signature numérique (on notera que tous ces documents doivent être enregistrés).

Il y a de nombreuses questions complexes dans les domaines des preuves, de l'autorité et de la responsabilité des notaires. Ces questions varient selon les juridictions et pour cette raison il est utile de demander des avis ou des examens juridiques.

7.5.1 Service de production de preuves

Pour produire des preuves, le TTP rassemble des informations relatives à un document, un message ou un événement lié à la sécurité d'un réseau ou d'un système, par exemple:

- a) l'identité des entités concernées;
- b) l'emplacement de ces entités;
- c) les données transférées;
- d) la méthode de transfert;
- e) l'horodatage.

La plupart de ces informations sont généralement celles qui permettent d'établir un journal d'audit.

Lorsqu'un TTP réunit, au nom d'entités, des données sur des événements liés à la sécurité, il peut établir une liste d'informations analogues sans indication du nom de l'origine des données pour des besoins d'analyse et d'étude dont les résultats seront communiqués à toutes les entités. Les détails relatifs à la collecte de ces données doivent être décrits dans des accords au niveau du service entre les entités participantes et le TTP.

7.5.2 Service de stockage de preuves

Conformément à l'ISO/CEI 13888-1, le service de stockage des preuves est combiné avec les services de transfert de recherche et des preuves. Les preuves stockées dépendent de la politique de sécurité en vigueur.

7.5.3 Service d'arbitrage

En cas de différend, et si celui-ci ne peut être résolu par les mécanismes et procédures de résolution appropriés du TTP, on peut recourir aux services d'un arbitre. Celui-ci doit réunir les preuves auprès des parties concernées et prendre ensuite une décision qui réglera le différend.

7.5.4 Autorité notariale

Une autorité notariale (NA, *notary authority*) est un TTP qui enregistre des données à un instant donné et qui peut vérifier l'exactitude des données spécifiques qui ont été enregistrées aux termes d'une politique de sécurité. Dans son rôle élémentaire, une NA agit en tant que service d'enregistrement et élargit son rôle lorsqu'elle agit en tant que service de validation. Ainsi le service de notaire peut contribuer à la fourniture du service de non-répudiation. Lorsque le notaire fait les vérifications, il ajoute les informations à ces données initialement enregistrées. Cela permet aux entités qui font confiance au notaire de s'assurer que ces données ont été vérifiées conformément à la politique de sécurité à un instant donné.

A titre d'exemple, un notaire peut authentifier un certificat conformément à une politique de sécurité. Dans ce cas, la NA s'assure que le certificat inclus dans la demande est valable, compte tenu de la politique de sécurité, et détermine son état de révocation à une heure donnée. Elle vérifie à nouveau le trajet de certification complet, de l'entité signant le certificat jusqu'à un point de confiance. La NA peut s'appuyer sur toutes les listes de révocation de certificats (CRL, *certificate revocation list*) et listes de révocation d'attributs (ARL, *attribute revocation list*) et, si nécessaire, les compléter par l'accès à des informations d'état plus courantes pour la CA. Elle inclut ces informations, ainsi qu'une heure fiable, pour créer un jeton notarial.

Autre exemple: un notaire peut authentifier une signature numérique conformément à une politique de sécurité. La NA vérifie la signature numérique et le trajet de certification conformément à la politique de sécurité. Dans ce cas, la validité et l'état de révocation du certificat de clé publique d'une entité ou de validité et le trajet de certification complet, de l'entité signataire jusqu'à un point de confiance (par exemple, la CA de la NA ou la CA racine dans une hiérarchie) seront vérifiés vis-à-vis de la politique de sécurité. La NA peut s'appuyer sur toutes les CRL et ARL qui s'appliquent et, si nécessaire, les compléter par l'accès à des informations d'état plus récentes émanant de la CA. Elle inclut une heure fiable et crée un jeton notarial.

Dernier exemple: un notaire peut authentifier des données formatées. La NA vérifie l'exactitude des données et crée un jeton notarial. Dans ce cas, cependant, "l'exactitude" des données n'est pas seulement axée sur la signature; la définition particulière qu'il convient d'appliquer est pour cette raison nécessairement dépendante de la politique de sécurité et du type de données. Les données proprement dites peuvent, par exemple, contenir une ou plusieurs signatures (dans ce cas "exactitude" se rapporte à la validité de ces signatures), peut contenir des assertions ("exactitude" se rapporte à la valeur réelle de ces déclarations), ou peut contenir un contrat ("exactitude" se rapporte à la validité juridique du document).

L'autorité notariale peut:

- a) vérifier l'exactitude de la signature numérique au moyen de toutes les informations d'état et des certificats de clés publiques appropriés et, si le demandeur le souhaite, produire un jeton notarial signé attestant la validité de la signature;
- b) vérifier la validité du certificat et son statut de révocation à l'heure spécifiée en utilisant toutes les informations d'état et certificats de clé publique appropriés, et produire un jeton notarial signé attestant la validité et l'état de révocation du certificat si le demandeur le souhaite;
- c) introduire une valeur incrémentielle monotone de l'heure ou un jeton horodateur dans son jeton notarial;
- d) introduire dans chaque jeton notarial signé un identificateur pour déterminer de manière unique la fiabilité et la politique de validation utilisée pour cette signature;
- e) signer chaque jeton notarial au moyen d'une clé produite exclusivement à cet effet et indiquer cette propriété de la clé sur le certificat correspondant;
- f) indiquer dans le jeton si la signature ou le certificat a été vérifié, et si tel n'est pas le cas, le motif du non-aboutissement de la vérification;
- g) si nécessaire, fournir un rapport signé (c'est-à-dire sous la forme d'un jeton notarial défini de manière appropriée) au demandeur, conformément à la politique.

D'autres précisions et un exemple de protocole de notaire figurent dans les protocoles de notaire IETF.

7.6 Service d'archivage numérique électronique

Un service d'archivage numérique électronique est un service fourni par un enregistreur de documents dans lequel sont enregistrés des documents électroniques afin de les sauvegarder et de les conserver en tant qu'archives permanentes. Parfois les documents électroniques doivent être enregistrés sous forme cryptée, surtout lorsque les données sont très sensibles et nécessitent une protection particulière.

Les opérations de base d'un service d'archivage sont:

- a) l'enregistrement des documents – le TTP peut conserver une version datée des documents dans un lieu de stockage sûr pendant un temps donné;
- b) la production de copies des documents – le service d'archivage publiera, sur la demande d'une entité agréée, une copie signée, avec la date d'enregistrement, des documents enregistrés.

L'authenticité des documents enregistrés dépend essentiellement des techniques cryptographiques telles que les signatures numériques.

L'archivage électronique d'un document pour une longue durée (plusieurs années) pour des raisons légales et juridiques doit tenir compte de quatre considérations de base:

- a) le support d'archivage nécessite éventuellement un rafraîchissement périodique (bande magnétique, CD-ROM, etc.);
- b) l'équipement technique pour accéder aux données archivées n'a pas nécessairement une durée de vie suffisante pour assurer l'accès aux données archivées pendant toute la durée voulue. Le changement d'équipement nécessitera des sauvegardes et le transfert des données archivées sur le nouveau support;
- c) pour interpréter correctement un document récupéré, il faut éventuellement fournir des informations additionnelles telles que le format de données (ASCII, Postscript ou HTML, par exemple), le nom de fichier et la date de création. Par ailleurs, il faut un logiciel exécutable acceptant le format;
- d) les algorithmes cryptographiques n'ont pas nécessairement une puissance suffisante pour parer aux agressions pendant la période d'archivage; si c'est le cas, il faut recourir à d'autres techniques de sécurité (par exemple la sécurité physique).

Une organisation peut également utiliser le service d'archivage (du point de vue des besoins de fonctionnement) pour la récupération des documents.

Un service d'archivage peut fonctionner comme un service de dépôt qui administre par fidéicommiss des documents électroniques pendant une durée déterminée. Un document ne doit pas être remis à d'autres entités tant que certaines conditions ne sont pas remplies. La politique de sécurité doit définir les circonstances dans lesquelles une entité peut avoir accès à ces documents, y compris l'interception mandatée ou légale (quand cela s'applique) ou l'accès par l'utilisateur ou l'entreprise. Un TTP est censé établir la liste de tous les documents en dépôt, par ordre chronologique.

Par exemple, si les entités A et B ont un accord contractuel par lequel l'entité A doit donner le code source du programme à un TTP pour l'administrer en fidéicommiss dans l'éventualité où l'entité A n'est plus en mesure de prendre en charge ou de maintenir à jour le programme. A une date ultérieure, l'entité B peut obtenir du TTP le code source du programme pour prendre en charge des fonctions commerciales qui seraient touchées.

7.7 Autres services

Le TTP peut fournir plusieurs autres services.

7.7.1 Service d'annuaire

Souvent les services de sécurité reposent sur des informations réelles et fiables, par exemple les certificats de clé publique, les listes de révocation de certification, les certificats d'attributs ou un extrait d'un registre commercial électronique fourni par l'annuaire.

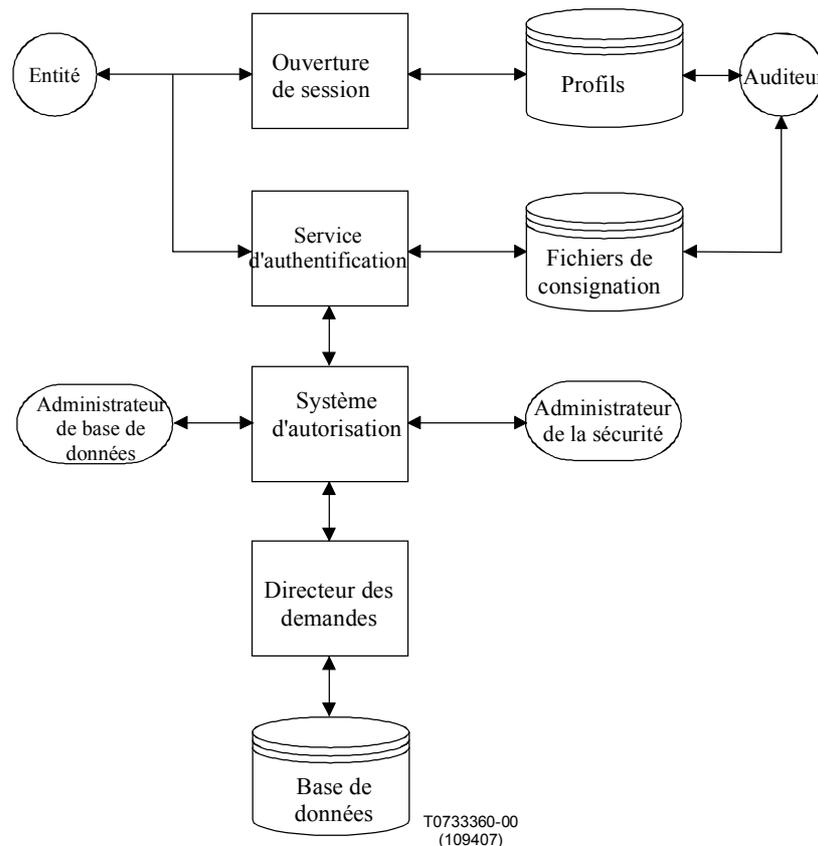


Figure 7 – Architecture du service d'annuaire

Avant qu'un service d'annuaire ne puisse être établi, il y a lieu d'identifier les objets en question en leur attribuant un nom. Pour identifier un objet sans équivoque, le nom – ou du moins l'ensemble d'objets concernés – doit être unique.

Une possibilité consiste à appliquer la dénomination OSI et l'adressage normalisé de la Rec. UIT-T X.650 | ISO/CEI 7498-3. Un exemple de service d'annuaire et des protocoles d'accès correspondants est illustré dans les Recommandations UIT-T de la série X.500 | ISO/CEI 9594. Après un accès correct, un service d'annuaire permet aux entités de demander des informations à la base de données (un ensemble de données enregistrées de manière permanente sur un support).

La Figure 7 représente l'ensemble d'une architecture de service d'annuaire. Après la prise de contact et une authentification positive, chaque demande de données adressée à l'annuaire est transmise par l'intermédiaire du système d'autorisation. Si les droits d'accès à l'entité sont conformes aux règles, l'accès est accordé; sinon, un message doit être envoyé à l'entité. Les tentatives d'accès qui n'ont pas abouti, par exemple les authentifications négatives, doivent être mises dans un fichier de consignation.

Le gestionnaire des demandes traite les demandes acceptées. Sa tâche consiste à compiler la demande, à accéder à la base de données et à donner la réponse à l'entité. Toutes les informations ne doivent pas nécessairement se trouver dans la même base de données locale.

Les rôles suivants interviennent dans la gestion de la sécurité d'un service d'annuaire:

- a) l'administrateur de la sécurité doit définir les règles d'autorisation compte tenu de la politique de sécurité; le choix de règles d'autorisation possibles est étendu, par exemple le service d'annuaire peut être ouvert au public ou limité à un groupe fermé d'utilisateurs qui rétribue le service;
- b) l'auditeur examine régulièrement le fichier de consignation pour détecter les transgressions de la sécurité ou les importuns;
- c) l'administrateur de la base de données assure la maintenance de la partie de l'annuaire qui contient les informations importantes pour la sécurité. Il a des droits d'accès et peut lire, écrire et supprimer des informations.

Les informations contenues dans l'annuaire peuvent être retrouvées de différentes manières:

- a) accès hors ligne: par cette méthode, la distribution automatique aux abonnés a lieu régulièrement; l'intervalle permet de déterminer à quel moment la mise à jour suivante aura lieu;
- b) accès en ligne: c'est la méthode de distribution à la demande des entités; un exemple courant est l'annuaire X.500.

7.7.2 Service d'identification et d'authentification

Dans un scénario habituel, où l'architecture répartie est constituée de clients et de serveurs répartis ou centralisés, une entité obtient l'accès à un serveur depuis une station de travail locale (le client). Dans cet environnement, la sécurité peut être assurée au moyen d'un service d'authentification qui est pris en charge par le TTP.

Ce service peut englober l'initialisation et la maintenance d'un service d'authentification ainsi que l'exploitation des équipements nécessaires tels qu'un serveur d'authentification. Ce service peut être fait en ligne ou hors ligne. On se référera à l'ISO/CEI 9798 pour les détails relatifs aux techniques d'authentification. D'autres prescriptions relatives à la sécurité, par exemple la protection des entités contre les usurpations d'identité, la protection de l'intégrité des données, de l'authenticité de leur origine et l'authentification réciproque entre entités, doivent être prises en compte.

Le service d'authentification peut porter sur les entités (utilisateurs) ou sur les données. Dans la plupart des cas, il doit être disponible en ligne. Il vérifie les certificats et les signatures, il peut utiliser un protocole d'authentification cryptographique ou un code d'authentification des messages (MAC) pour rétablir la preuve de l'origine ou la preuve de remise des données.

L'implémentation la plus courante d'un service d'authentification est le service Kerberos d'attribution de tickets (pour des informations additionnelles, se référer à Steiner *et al.*: Kerberos: an authentication service for open network systems in the proceeding winter 1988 USENIX Conference, pages 191-202).

7.7.2.1 Service d'authentification en ligne

Lorsqu'un grand nombre d'entités souhaitent communiquer, un service d'authentification entre homologues peut faire appel à un TTP pour éviter que chaque entité soit dans l'obligation de disposer des informations d'authentification de toutes les autres. L'entité en ligne participe à chaque opération d'authentification. Le TTP peut authentifier l'entité A et lui fournir un certificat qu'il doit présenter à l'entité B, ou il peut vérifier l'information d'authentification de l'entité A reçue par l'entité B au nom de celle-ci.

Les systèmes d'authentification symétriques nécessitent que chaque entité qui souhaite être authentifiée partage une clé secrète avec chaque autre entité. Plutôt que de produire et de distribuer un grand nombre de clés [$n(n - 1)/2$ clés pour un groupe de n entités], on pourrait utiliser un service d'authentification en ligne pour réduire ce nombre. Le résultat serait:

- a) que seul le TTP qui assure le service d'authentification partage une clé secrète avec chaque entité;
- b) que chaque entité partage une clé secrète avec le TTP.

Deux méthodes générales sont possibles:

- a) la méthode du jeton. Avant que l'entité ne puisse s'authentifier, elle peut demander un jeton à un TTP. Ce jeton est utilisé dans la procédure d'authentification détaillée plus loin;
- b) l'entité qui souhaite être authentifiée envoie directement un message scellé; étant donné que le vérificateur n'a pas de moyen (n'a pas de clé commune) de valider ce message, le TTP s'en charge au nom du vérificateur et lui notifie le résultat.

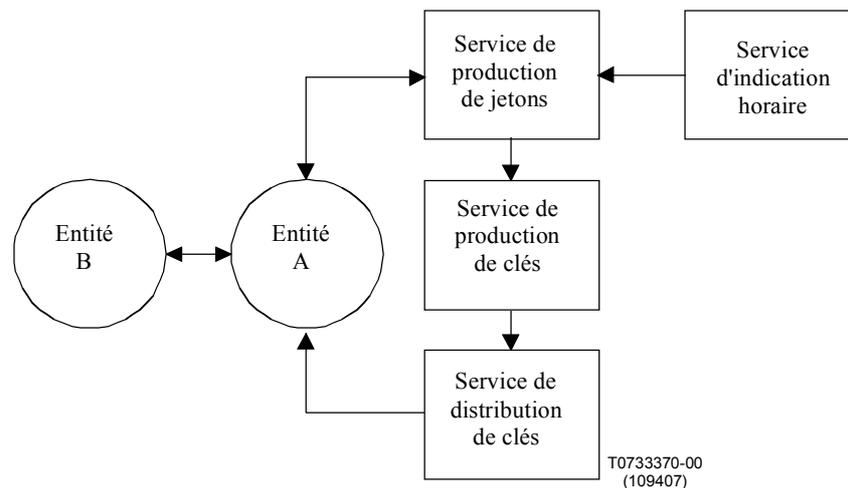


Figure 8 – Exemple de services d'authentification en ligne

La Figure 8 représente le modèle général de service d'authentification en ligne. Un tel service comporte deux phases:

- a) la phase d'initialisation: au cours de celle-ci, les principales tâches pourraient être l'identification correcte des entités et la fourniture de clés;
- b) la phase d'exécution: on part de l'hypothèse que l'utilisateur, l'entité A, doit s'authentifier vis-à-vis du TTP local fournissant des services d'authentification. Ce service fournit à A les titres nécessaires pour accéder à l'utilisateur distant, l'entité B.

En principe, ce service peut s'effectuer en diverses étapes, dont chacune peut être constituée de plusieurs échanges de messages. Si l'entité A souhaite accéder à une application ou un service assuré par l'entité B, l'entité A pourrait procéder aux étapes 1 et 2:

- 1) l'étape A envoie une demande au fournisseur de services d'authentification avec son moyen d'authentification (par exemple un mot de passe, un jeton d'authentification produit au moyen d'une carte à puce) et demande ses "lettres de créance";
- 2) le fournisseur du service d'authentification vérifie les droits d'accès de A et, si les conditions sont remplies, répond au moyen d'un jeton qui permet à l'entité de s'authentifier elle-même et d'avoir accès au serveur pour l'application demandée sur le site de l'entité B. Ce jeton peut contenir une indication horaire, une clé de session, des éléments cryptographiques pour l'authentification et, facultativement, d'autres éléments.

Les étapes 3 et 4 ne font pas intervenir directement le fournisseur du service d'authentification, mais le jeton qui accorde à l'entité A l'accès au service de l'entité B doit être choisi en fonction de la clé qui est partagée par le fournisseur du service d'authentification et l'entité B.

- 3) le jeton est envoyé de l'entité A à une entité B distante, qui vérifie le jeton reçu. Ce jeton a dû être choisi en fonction de la clé commune à l'entité B et au fournisseur du service d'authentification. Si c'est le cas, l'entité B autorise l'accès au service demandé;
- 4) facultativement, si une authentification mutuelle est requise, l'entité B doit s'authentifier vis-à-vis de l'entité A de la même manière que celle employée précédemment par l'entité A.

Un exemple d'un tel service d'authentification est donné dans RFC 1510.

7.7.2.2 Service d'authentification hors ligne

Les services d'authentification hors ligne s'appuient principalement sur des techniques asymétriques en combinaison avec des services de gestion des certificats.

Le TTP hors ligne produit et distribue à l'avance des certificats d'authentification hors ligne que l'entité B peut utiliser ultérieurement pour valider un échange d'authentification. Ce certificat d'authentification peut être stocké à l'avance par l'entité B ou envoyé par l'entité A, avec l'information d'authentification (AI, *authentication information*), au moment où l'authentification a lieu. Il peut également être stocké dans un centre d'information où B peut le retrouver en cas de nécessité.

L'authentification hors ligne utilisant le TTP est généralement associée au concept d'autorité de certification. On trouvera d'autres précisions à ce sujet dans l'ISO/CEI 9798-1 et ISO/CEI 11770-1.

7.7.2.3 Service d'authentification en ligne

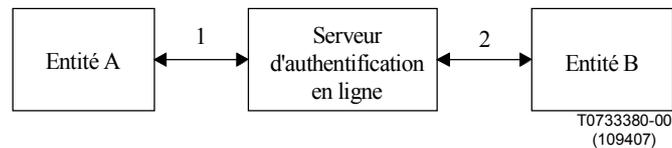


Figure 9 – Exemple de service d'authentification TTP en ligne

Dans cet exemple, le serveur d'authentification du TTP est placé sur le trajet de communication entre les deux entités, comme le montre la Figure 9. Le processus d'authentification comprend deux étapes, chacune pouvant être constituée de plusieurs échanges de messages.

En premier lieu, l'entité A tente de s'authentifier auprès du TTP et, si cela aboutit, le TTP s'authentifie auprès de l'entité B et se porte garant de l'identité de l'entité A, y compris une authentification entre le TTP et l'entité B.

7.7.3 Service de transposition en ligne

Lorsque les deux entités appartiennent à des domaines de politique de sécurité différents, le TTP doit transposer la politique d'authentification du domaine cible en celle du domaine d'origine, par exemple en termes de puissance du mécanisme d'authentification qu'il convient d'utiliser. Ce système peut également être constitué d'une suite de TTP formant un lien entre les deux entités.

7.7.4 Services de récupération

Ces services sont facultatifs et ne sont pas couramment proposés comme services séparés mais en combinaison avec d'autres services qui peuvent être proposés dans le cadre des activités quotidiennes.

7.7.4.1 Services de récupération de clé

La récupération, la mise en dépôt et l'encapsulation de clé sont des fonctions d'un système cryptographique fournissant une capacité de décryptage de secours qui permet aux entités autorisées, dans certaines conditions, de décrypter des données au moyen d'informations fournies par un ou plusieurs TTP (dans ce contexte, de confiance signifie "ayant la confiance tant de l'utilisateur que de l'entité autorisée").

L'expression "récupération de clé" est utilisée de différentes manières selon le contexte. Elle est, par exemple, utilisée dans certains contextes comme terme générique couvrant à la fois les systèmes de mise en dépôt ou les systèmes d'encapsulation. Dans d'autres, elle signifie la mise en dépôt ou l'encapsulation proprement dit.

- Clé en dépôt: dans un système cryptographique utilisant des clés en dépôt, une copie d'une clé secrète, ou le moyen de la produire, est soit détenue par un TTP autorisé, soit divisée en deux ou plusieurs parties détenues par plusieurs TTP autorisés. En vertu de la législation nationale, les TTP mettent une telle clé ou de telles parties de clé à la disposition des entités autorisées.
- Encapsulation de clé: dans un système cryptographique utilisant l'encapsulation de clé, les paramètres permettant de reconstruire la clé sont joints aux données cryptées ou logiquement associés aux données cryptées mais acheminés et stockés dans un emplacement physiquement séparé. En vertu de la législation nationale, le système cryptographique permettrait à un tiers de reconstituer une clé sur demande avec l'aide des informations fournies par un ou plusieurs TTP autorisés. Dans le cas de l'encapsulation, les TTP ne détiennent pas directement la clé ou des parties de clé mais les informations indispensables au processus de reconstitution.

NOTE – Les différences entre les divers systèmes dépendent principalement des détails d'implémentation, de l'infrastructure (c'est-à-dire des fonctions et responsabilités attribuées aux TTP) et des arrangements institutionnels fixés par la législation nationale. Quel que soit le système, dès que la copie d'une clé secrète est reconstituée ou transmise à un tiers, elle ne peut plus être considérée comme étant secrète. Par exemple, toutes les communications et données enregistrées cryptées à l'aide de cette clé pourraient éventuellement être décryptées. La récupération de la clé, la mise en dépôt et l'encapsulation ne devraient être utilisés que pour des clés de confidentialité.

Les services de récupération de clé permettent le décryptage des données, que celles-ci soient en cours de communication ou stockées. Des domaines d'application courants sont notamment l'interception légale (quand elle s'applique) ainsi que l'accès utilisateur/entreprise. La principale différence entre ces domaines d'application sont les conditions prescrites dans lesquelles le décryptage du texte chiffré peut avoir lieu.

Par exemple, une organisation peut choisir d'exploiter un service de récupération pour fournir des clés permettant de récupérer des fichiers commerciaux et d'information d'une entreprise qui ont été cryptés par des employés. Les clés sont employées pour des décryptages d'urgence ayant pour but de récupérer des données cryptées au moyen de clés qui ont été perdues ou endommagées.

Il existe un besoin pour des mécanismes de contrôle d'accès sévères par lesquels seules des personnes autorisées, identifiées et authentifiées, ayant réellement besoin de savoir, peuvent accéder aux clés. Pour augmenter la fiabilité des clés, elles peuvent être stockées sous forme cryptée à plusieurs endroits différents.

Lorsqu'il assure des service de récupération de clé, le TTP pourrait combiner les rôles de producteur de clés et d'agence de distribution pour ses utilisateurs ainsi que de fournisseur de clés d'utilisateur. Un TTP offrant de tels services devrait également s'occuper de questions telles que la révocation des clés, leur stockage, leur récupération et leur reconstitution.

7.7.4.2 Services de récupération de données

Ce service peut être assuré au moyen de l'un des deux systèmes de base suivants:

Le premier type de système se caractérise par des clés privées ou secrètes associées à des entités en cours d'enregistrement auprès d'un ou de plusieurs TTP avant que les données ne soient cryptées pour communication ou stockage. Ces informations relatives aux clés peuvent être utilisées plus tard pour récupérer les données, conformément aux dispositions contractuelles ou légales.

Le second type de système se caractérise par un individu utilisant des clés publiques se rapportant à un ou plusieurs TTP pour crypter des données en vue de leur communication ou de leur stockage. La procédure de cryptage est telle qu'elle permet le décryptage par le destinataire visé. Il permet la récupération des données conformément aux prescriptions contractuelles et légales au moyen de clés privées, détenues par un ou plusieurs TTP, et des informations associées à ces données cryptées.

7.7.5 Service de personnalisation

Le service de personnalisation comprend le cryptage d'éléments cryptographiques sûrs dans des jetons de sécurité, par exemple des cartes à puce. Les éléments cryptographiques englobent notamment des clés secrètes, des clés publiques, des certificats et des nombres aléatoires. Ils doivent être inscrits dans un environnement inaltérable, et doivent être accessibles aux entités destinataires, identifiées et authentifiées, seulement. Ce service doit fournir un registre des jetons personnalisés et des détenteurs agréés.

7.7.6 Service de contrôle d'accès

Un TTP en ligne a la capacité de fournir des informations de contrôle d'accès de la même manière qu'il fournit des informations d'authentification lorsqu'une entité agréée les lui demande. Il agit comme un service de certification pour les "privilèges" de contrôle d'accès d'une entité afin d'assurer que les ressources d'un système de gestion de clés ne soient accessibles qu'aux entités agréées et de manière autorisée. On trouvera des précisions à ce sujet dans l'ISO/CEI 11770-1. Le TTP de contrôle d'accès en ligne est appelé un serveur de contrôle d'accès.

7.7.7 Service de signalisation des incidents et de gestion des alertes

En vertu de l'ISO/CEI TR 13335, une politique de sécurité IT doit être examinée régulièrement et maintenue à jour compte tenu d'un environnement changeant rapidement. Il faut des procédures pour traiter d'événements de sécurité spécifiques détectés par ou portés à l'attention du TTP qui signale les incidents et gère les alertes. Ce service peut être traité manuellement ou automatiquement.

S'il se produit un incident tel qu'une fraude, les informations détaillées correspondantes sont signalées à l'entité responsable des incidents (ou bien celle-ci détecte elle-même l'incident):

- a) soit par l'une des entités, qui envoie un message d'alerte au TTP;
- b) le TTP peut recevoir automatiquement des informations relatives à un événement, par exemple en localisant la communication ou en demandant des informations à d'autres entités, par exemple en cas de détection par suite de l'absence de disponibilité.

Un tel incident produit un impact sur l'organisation concernée; il nécessite un examen et une étude pour trouver des solutions qui annuleront ou diminueront les effets d'une répétition de l'incident.

Lorsqu'une entité rend compte d'un incident à son TTP, celui-ci doit fournir des services de gestion d'alerte à d'autres entités comme prévu par les accords de service.

De plus, toutes les informations pertinentes relatives aux événements (l'occurrence, les effets et la suite donnée) doivent être indiqués afin que l'analyse et l'étude puissent se poursuivre. Une information d'alerte peut avoir pour résultat des actions de gestion telles que la transmission de messages d'alerte à d'autres entités ou éventuellement à d'autres TTP. Une raison pourrait être que la clé privée d'une autorité de certification ou la clé privée (secrète) d'une entité soit compromise.

Il peut se produire que des entités aimeraient partager/avoir accès à des informations globales au sujet des risques liés à la sécurité, aux faiblesses, aux incidents ou aux événements dans leur secteur d'activité. Toutefois, ces entités ne souhaitent guère partager ces informations lorsque celles-ci peuvent donner un aperçu de leur propre système de sécurité ou diminuer le niveau de la confiance des clients. Un TTP peut rendre service à des entités dont les informations ont été réunies, analysées et partagées avec d'autres, conformément aux accords de service en vigueur. La Figure 10 montre un exemple de TTP qui peut collecter des informations d'incidents relatifs à la sécurité émanant d'une entité pour ensuite, sans identifier l'entité en question, partager ces informations avec toutes les autres. Le TTP peut également réunir directement des informations de toutes les entités pour les analyser et partager ensuite les résultats avec toutes les entités.

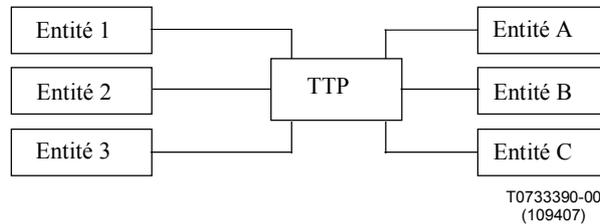


Figure 10 – Exemple de service de gestion des alertes

Annexe A

Prescriptions de sécurité pour la gestion des TTP

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Rapport technique)

Concrètement, il conviendrait de faire une évaluation pour déterminer le niveau de risque associé aux services de TTP qu'il y a lieu de mettre en œuvre. Le type et le niveau des prescriptions de sécurité à sélectionner dépendront des services spécifiques fournis par le TTP et des risques encourus au cas où les services du TTP seraient compromis. Les prescriptions de sécurité associées à ces risques identifiés doivent être spécifiées dans la politique de sécurité du TTP. L'évaluation et l'élaboration de la politique doivent englober ce qui suit:

- a) les utilisateurs, les administrations et le personnel d'exploitation du TTP ne doivent avoir accès qu'aux informations et aux ressources auxquelles ils ont droit;
- b) les procédures administratives doivent permettre l'identification exclusive et sûre ainsi que l'enregistrement des utilisateurs et des opérateurs des services du TTP;
- c) les éléments très délicats, qui sont fondamentaux pour la confiance pouvant être placée dans le TTP, la clé privée de l'autorité de certification (CA) ou la clé du niveau supérieur d'un centre de distribution de clés, par exemple, doivent être produites, mises en place et gérées conformément à des procédures dûment étayées et fiables;
- d) pour assurer la traçabilité des opérations et des transactions et la fiabilité des entités, il convient de prendre les mesures suivantes avec l'autorité voulue:
 - 1) l'authentification des entités;
 - 2) la signature électronique de toutes les demandes, transactions et opérations sensibles au plan de la sécurité;
 - 3) restreindre les résultats d'audit aux autorités compétentes (par exemple les auditeurs);
- e) afin de protéger la confidentialité des intérêts commerciaux de toutes les entités concernées, les informations aboutissant aux interfaces, acheminées par des protocoles ou sur des supports de stockage, doivent représenter le niveau requis d'intégrité et de protection de la confidentialité;
- f) la sécurité du système, y compris la sécurité du système d'exploitation, de toutes les composantes régies par la politique de sécurité du TTP doit garantir la protection nécessaire dans les conditions d'exploitation réelles;
- g) une gestion adéquate de la sécurité doit englober le lancement, la surveillance et le contrôle des services de sécurité qui protègent les services fournis par le TTP;
- h) les procédures doivent permettre de rétablir une situation sûre après une atteinte à la sécurité. Cela sous-entend également la récupération ou le remplacement de la ou des clés secrètes de niveau supérieur du TTP;
- i) des mécanismes doivent être mis en place pour se protéger contre tout point faible individuel pouvant survenir dans des systèmes où le TTP est en mesure de récupérer les données cryptées par la récupération de la clé;
- j) si nécessaire en raison de la politique de sécurité des entités concernées, le TTP doit fournir les moyens d'assurer que seules les clés requises par une entité autorisée peuvent être récupérées par le TTP; et
- k) les procédures de récupération doivent également limiter autant que possible les effets sur l'entité au moyen des procédures de notification appropriées.

Annexe B

Questions relatives à la gestion des autorités de certification

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Rapport technique)

B.1 Exemple de procédure de processus d'enregistrement

La CA est chargée d'entreprendre les procédures requises pour établir que le demandeur du certificat est le ou la personne prétendue. Dans des circonstances particulières, la CA peut autoriser une autre entité nommée autorité d'enregistrement (RA) à effectuer l'enregistrement de l'abonné au nom de la CA.

Le processus d'inscription de l'abonné peut être déclenché par le candidat (la personne qui veut s'abonner) la CA, la RA ou un responsable de l'administration qui coordonne l'établissement d'un réseau organisationnel.

La CA (RA) doit s'assurer que tout demandeur de certificat a le droit d'obtenir un tel certificat et, si le certificat implique que l'abonné bénéficie d'attributs ou de privilèges particuliers, que ceux-ci sont réels.

La relation entre un abonné et un employeur ainsi que l'approbation par ce dernier de l'émission d'un certificat pour l'abonné doivent être attestées par un représentant légitime de l'employeur.

Dans son accord avec l'employeur, la CA doit s'assurer que celui-ci se charge de l'informer des changements significatifs de l'état de l'emploi au cours de la période de validité des certificats émis.

Le ou la candidate doit se présenter en personne à la CA, à la RA ou à un représentant désigné de la CA pour être authentifié ou authentifiée avant l'émission du certificat, cela indépendamment du fait que l'abonné est indépendant ou associé à un employeur. Cela ne peut être traité directement par l'employeur que si lui-même est une CA ou une RA désignée par la CA.

Le candidat doit présenter des papiers d'identification valables. Une indication relative aux moyens d'identification doit être donnée sur le formulaire pour attester que la vérification a effectivement eu lieu.

Lorsqu'il authentifie un candidat, l'abonné doit présenter à la CA ou à la RA un document d'identification avec photographie, certifié et couramment admis, tel qu'une carte d'identité nationale, la personne responsable à la CA ou celle qui la représente à la RA ayant signé.

Si le candidat ne possède pas le document d'identification avec photo dont il est question ci-dessus, il peut soumettre un document officiel authentifiant l'identité revendiquée, en présence d'une personne neutre d'âge mûr, authentifiée comme indiqué ci-dessus, qui certifie que l'identité du candidat est celle revendiquée.

Les détails relatifs à l'individu, tels que des identificateurs uniques, le nom et l'adresse connus, doivent être comparés avec les informations d'un registre officiel ou d'une autre organisation ou tiers bénéficiant de la confiance de la CA à cet effet.

B.2 Exemple de conditions à remplir par les autorités de certification

Une autorité de certification (CA) qui émet des certificats doit le faire en conformité avec une politique appropriée en la matière. En vertu de celle-ci, elle doit veiller au minimum:

- a) à fournir des services de certification et de référentiel compatibles entre eux;
- b) à fournir des directives concernant les prescriptions d'exploitation;
- c) à effectuer les procédures d'authentification relatives aux demandes d'enregistrement initiales et de révocation;
- d) à émettre des certificats conformément à la politique définie en matière de certificats et à honorer les diverses représentations aux abonnés et aux parties concernées présentées dans une déclaration relative aux méthodes de certification (CPS – Certification Practice Statement, qui est une déclaration relative aux méthodes employées par une autorité de certification pour émettre des certificats);
- e) à s'associer aux droits des abonnés et des parties concernées qui utilisent des certificats en conformité avec les lois et les règlements applicables;

- f) à révoquer des certificats et à publier des listes CRL relatives à la définition de la politique en matière de certificats (la suppression des certificats est une décision de l'autorité de certification);
- g) à être conforme aux dispositions définies dans sa politique en matière de certificats et aux dispositions légales éventuelles, publiées dans une déclaration CPS.

La CA est responsable de tous les engagements énumérés ci-dessus, qu'ils soient ou non effectués par la CA ou par une autorité d'enregistrement (RA) nommée par la CA. Les engagements de la CA vis-à-vis de toutes les entités extérieures englobent pour cette raison tous les engagements pris par la RA.

Les CA doivent prendre des engagements additionnels suivants:

- a) *relatifs à l'émission de la clé privée de la CA*
une CA doit protéger sa clé privée conformément à certaines dispositions décrites dans la politique des certificats;
- b) *relatifs aux restrictions d'utilisation de la clé privée de la CA*
la clé privée d'une CA utilisée pour l'émission de certificats qui sont conformes à la présente politique en matière de certificats doit être utilisée uniquement pour la signature des certificats et, facultativement, des listes CRL et autres informations appropriées cadrant avec l'émission des certificats.

Si une CA s'engage à agir en conformité avec d'autres politiques en utilisant la même clé privée ou identité d'émission, elle doit le spécifier dans la déclaration CPS.

Une RA est une entité chargée de l'identification et de l'authentification d'entités de certificats de clé publique, mais elle n'est pas une CA ou une AA et pour cette raison n'assigne ou n'émet pas de certificats. Une RA peut aider dans le processus d'application des certificats, le processus de révocation ou les deux. La RA ne doit pas être un organe séparé, elle peut faire partie de la CA.

Compétences pouvant être attribuées à une RA:

- a) valider l'identité de l'entité demandant un certificat de clé publique, conformément à la déclaration de méthode de certification (CPS, *certification practice statement*) de la CA;
- b) certifier que l'identité de l'entité demandant le certificat est l'entité certifiée par le certificat. A cet effet, elle peut faire signer la demande de certificat par l'entité et faire valider cette signature par la RA au moyen de la clé publique présentée pour certification;
- c) enregistrer de manière sûre les entités authentifiées;
- d) notifier à l'entité identifiée dans le certificat la confirmation de l'enregistrement et l'émission du certificat;
- e) tenir à jour des dossiers d'audit à l'appui des certificats qu'elle émet pendant la période déterminée par la prescription en matière de conservation des enregistrements;
- f) donner des orientations à ses abonnés sur la gestion sûre de leur clé privée;
- g) utiliser tout moyen approprié pour assurer que l'entité identifiée dans le certificat est consciente de ses responsabilités et qu'elle est capable de s'y conformer;
- h) informer les entités du domaine en cas de compromission de la clé privée de la CA;
- i) traiter les demandes de révocation des certificats émanant des entités;
- j) informer l'entité identifiée dans le certificat que l'intégrité de ses activités sera jugée compromise si sa clé privée devait être révélée à une entité non autorisée ou utilisée par une telle entité; et
- k) veiller à maintenir une gestion saine et des méthodes de contrôle qui seront confirmées par des processus de procédure d'assurance qualité en matière de sécurité et des audits de conformité indépendants.

Une RA ayant des activités liées à l'établissement de certificats doit au minimum s'engager:

- a) à établir les moyens nécessaires pour répondre aux conditions d'utilisation figurant dans la politique définie en matière de certificats;
- b) à exécuter les procédures d'authentification conformément aux règles spécifiées dans la politique définie en matière de certificats;
- c) à tenir les engagements pris, à défendre les droits des abonnés et des parties concernées qui utilisent les certificats conformément aux lois et règlements fédéraux, d'Etat ou provinciaux;

- d) à se conformer à toutes les dispositions relatives aux obligations, à la responsabilité financière, aux taxes, aux publications et aux référentiels, à l'audit de conformité, à la confidentialité, aux droits de propriété intellectuelle, aux accords contractuels précisés dans la politique définie en matière de certificats et toute disposition légale, dispositions réunies dans une déclaration CPS imprimée.

Par ailleurs, les RA peuvent être obligées par la loi à donner d'autres garanties.

La RA doit en outre:

- a) protéger sa clé privée conformément aux dispositions de la politique en matière de certificats;
- b) ne pas utiliser à toute autre fin, sans l'autorisation expresse de la CA, les clés privées destinées à des fins associées à sa fonction de RA;
- c) restreindre l'utilisation des clés privées de la RA conformément aux prescriptions d'utilisation figurant dans les certificats associés.

L'abonné a également certaines obligations qui doivent figurer dans l'accord entre la CA et l'abonné conformément aux accords contractuels, à savoir:

- a) l'abonné doit s'engager à suivre certaines procédures lorsqu'il fait une demande de certificat;
- b) l'abonné doit conserver le contrôle de sa clé privée et la protéger conformément aux parties applicables de la politique définie en matière de certificats et prendre les précautions raisonnables pour empêcher sa perte, sa divulgation à des tiers, sa modification ou son utilisation non autorisée;
- c) l'abonné doit signaler à la CA toute suspicion d'atteinte à l'intégrité de la clé;
- d) le jeton cryptographique, sur lequel sont enregistrées les clés privées, doit être protégé dans une mesure qui s'apparente à celle d'objets personnels de valeur, de cartes de crédit ou de permis de conduire. Le code PIN ou le mot de passe permettant de débloquer le jeton ne doit jamais être placé au même endroit que le jeton;
- e) les abonnés ne doivent pas laisser leur jeton cryptographique sans surveillance à l'état débloqué (c'est-à-dire sans surveillance dans un lieu de travail lorsque le code PIN ou le mot de passe a été entré).

B.3 Politique de certification et déclaration relative aux méthodes de certification (CPS)

Lorsqu'une autorité de certification émet un certificat, elle remet à un utilisateur du certificat (c'est-à-dire une partie concernée) une déclaration selon laquelle une clé publique donnée est liée à une entité donnée (le sujet du certificat). Toutefois, l'utilisateur du certificat doit évaluer lui-même la mesure dans laquelle il doit se fier à cette déclaration. Des certificats différents sont émis selon les méthodes et procédures et peuvent être adaptés à des applications ou des objectifs différents.

La Rec. UIT-T X.509 | ISO/CEI 9594-8 définit la politique de certification comme étant un "ensemble nommé de règles qui indique l'applicabilité d'un certificat à une communauté particulière ou à une classe d'application particulière ayant des exigences de sécurité communes". Un certificat X.509 Version 3 peut contenir une indication de la politique de certification qui peut être utilisée par l'utilisateur du certificat pour décider s'il doit se fier ou non à un certificat dans un but donné.

Une politique de certification qui doit être reconnue à la fois par l'émetteur et l'utilisateur d'un certificat est représentée dans un certificat par un identificateur d'objet unique, agréé. Le processus d'enregistrement suit les procédures spécifiées dans les Recommandations | Normes internationales de l'UIT-T. La partie qui enregistre l'identificateur d'objet public évalue également une spécification sous forme de texte de la politique de certification en vue de son examen par les utilisateurs des certificats. Un tel certificat définit généralement une seule politique de certification ou sera, si possible, compatible avec un petit nombre de politiques différentes.

Les politiques de certification constituent également une base pour la certification mutuelle des CA accompagnée d'une déclaration relative à la méthode de certification (CPS). Chaque CA est certifiée vis-à-vis d'une ou plusieurs politiques de certification qu'elle est censée mettre en œuvre. Lorsqu'une CA émet un certificat de CA pour une autre CA, la première doit évaluer l'ensemble des politiques de certification pour lesquelles elle fait confiance à la seconde (une telle évaluation doit être fondée sur la certification vis-à-vis des politiques de certification concernées). L'ensemble évalué de politiques de certification est ensuite indiqué par la CA émettrice dans un certificat CA. La logique de traitement du chemin de certification X.509 utilise les indications des politiques de certification dans son modèle de confiance clairement défini. Les notions de politique de certification et de déclaration CPS émanent de sources différentes et ont été élaborées pour des raisons différentes. Toutefois, leur corrélation est importante.

Une CPS est une déclaration détaillée faite par une CA au sujet de ses méthodes, déclaration qui doit potentiellement être comprise et consultée par les abonnés et les utilisateurs de certificats (parties concernées). Bien que le niveau de précision puisse varier entre les CPS, ils sont généralement plus détaillés que les politiques de certification. Une déclaration CPS peut être un document très complet, solide, donnant des descriptions exactes des offres de service, des procédures détaillées de la gestion des certificats sur toute leur durée de vie, voire au-delà, au niveau des détails qui destinent la CPS à une réalisation particulière (propriétaire) d'une offre de service.

Les précisions données dans une CPS sont nécessaires pour évaluer totalement la fiabilité en l'absence d'accréditation ou d'autres moyens de mesure de la qualité connus. Le CPS détaillé n'est pas, à lui seul une base suffisante pour l'interopérabilité entre des CA exploitées par des organisations différentes. Les politiques de certification sont plutôt le véhicule permettant aux parties concernées de déterminer si un certificat donné convient à leurs applications ou leurs objectifs. Une CA ayant une seule CPS peut prendre en charge plusieurs politiques de certification (utilisées pour diverses applications ou par différentes communautés d'utilisateurs de certificat). De même, plusieurs CA différentes ayant des CPS qui ne sont pas identiques peuvent prendre en charge la même politique de certification.

Voir aussi RFC 2527, Certificate Policy and Certification Practices Framework, S. Chokhani, W.Ford, mars 1999.

Annexe C

Bibliographie

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Rapport technique)

Référence normatives

- AS/NZS 4444, Australian/New Zealand Standard Code of Practice.
- BS 7799, British Standard Code of Practice – Révision 1, 1999.
- ETSI EG/SEC-003000, *Requirements for Trusted Third Party Services* (Edition 1), version 7.0, juillet 1997.
- FIPS PUB 140-1, Federal Information Processing Standard Publication 140-1, Security Requirements for Cryptographic Modules, U.S. Department of commerce, National Institute of Standards and Technology, janvier 1994.
- ISO/CEI Guide 61:1996, *Exigences générales pour l'évaluation et l'accréditation d'organismes de certification/d'enregistrement*.
- ISO/CEI Guide 65:1996, *Exigences générales relatives aux organismes procédant à la certification de produits*.
- ISO/CEI 9798-2:1999, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques*.
- ISO/CEI 9798-3:1998, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 3: Mécanismes utilisant des techniques de signatures numériques*.
- ISO/CEI 9798-4:1999, *Technologies de l'information – Techniques de sécurité – Authentification d'entité – Partie 4: Mécanismes utilisant une fonction cryptographique de vérification*.
- ISO/CEI 10118-1:2000, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 1: Généralités*.
- ISO/CEI 10118-2:2000, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 2: Fonctions de brouillage utilisant un chiffrement par blocs de n bits*.
- ISO/CEI 10118-3:1998, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 3: Fonctions de hachage dédiées*.
- ISO/CEI 13888-1:1997, *Technologies de l'information – Techniques de sécurité – Non-répudiation – Partie 1: Généralités*.
- ISO/CEI 13888-3:1997, *Technologies de l'information – Techniques de sécurité – Non-répudiation – Partie 3: Mécanismes utilisant des techniques asymétriques*.
- ISO/CEI 15408-1:1999, *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI – Partie 1: Introduction et modèle général*.
- ISO/CEI 15408-2:1999, *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI – Partie 2: Exigences fonctionnelles de sécurité*.
- ISO/CEI 15408-3:1999, *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI – Partie 3: Exigences d'assurance de sécurité*.
- ISO TC68 SC2 15782-1, *Banking – Certificate Management Part 1: Public Key Certificates*.
- ISO/CEI 15945, *Technologies de l'information – Techniques de sécurité – Spécifications des services de tiers de confiance TTP pour la prise en charge des applications de signature numérique*.
- ISO/CEI 15946-3, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques – Partie 3: Établissement de clé*.
- Recommandation UIT-T X.520 (2001) | ISO/CEI 9594-6:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés*.
- Recommandation UIT-T X.650 (1996) | ISO/CEI 7498-3:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: dénomination et adressage*.
- Recommandation UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base*.

- Recommandation UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels.*
- Recommandation UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes.*
- Recommandation UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*
- Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification.*
- Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès.*
- Recommandation UIT-T X.814 (1995) | ISO/CEI 10181-5:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité.*
- Recommandation UIT-T X.815 (1995) | ISO/CEI 10181-6:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité.*
- ITSEC, *Information Technology Security Evaluation Criteria (ITSEC)*, Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, version 1.2, juin 1992.
- NIST, *Computer Security Handbook.*
- NIST, *Minimum Interoperability Specification for PKI Components (MISPC)*, 1997.
- PKIX Part V, Internet X.509 Public Key Infrastructure, Internet Draft, Time Stamp Protocols, C. Adams, P. Cain, D. Pinkas, R. Zuccherato, mars 2000 (en cours).
- PKIX Part VI, Internet X.509 Public Key Infrastructure, Internet Draft, Data Certification Server Protocols, C. Adams, Sylvester, Zolotarev, R. Zuccherato, mars 2000 (en cours).
- RFC 1421, *Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures*, février 1993.
- RFC 1422, *Privacy Enhancement for Internet Electronic Mail: Part 2: Certificate-Based Key Management*", février 1993.
- RFC 1423, *Privacy Enhancement for Internet Electronic Mail: Part 3: Algorithms, Modes, and Identifiers*, février 1993.
- RFC 1424, *Private Enhancement for Internet Electronic Mail: Part 4: Key Certification and Related Services*, février 1993.
- RFC 1510, *The Kerberos Network Authentication Services*, septembre 1993.
- RFC 1750, *Randomness Recommendations for Security*, décembre 1994.
- RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, janvier 1999.
- RFC 2510, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, mars 1999.
- RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, mars 1999.
- RFC 2559, *Internet X.509 Public Key Infrastructure Operational Protocols – LDAPv2*, avril 1999.
- S2101/02, *Report to the Commission of the European Communities for the "Code of Practice and Management Guidelines for Trusted Third Party Services"*, version 1.0, 1993.
- SAA MP75-1996, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia.*
- STEINER et al.: Kerberos: an authentication service for open network systems in the proceeding winter, *USENIX Conference*, pages 191-202, 1988.

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	Réseaux câblés et 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	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie 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 de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication