RAPPORT TECHNIQUE

# ISO/CEI TR 14516

Première édition
2002-06-15

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

*Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*



Numéro de référence
ISO/CEI TR 14516:2002(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

# TABLE DES MATIÈRES


*Page*

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'horodalage ..... 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

*Page*

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

# Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 3.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

Exceptionnellement, le comité technique mixte peut proposer la publication d'un rapport technique de l'un des types suivants:



— type 1: lorsque, en dépit de maints efforts, l'accord requis ne peut être réalisé en faveur de la publication d'une Norme internationale;

— type 2: lorsque le sujet en question est encore en cours de développement technique ou lorsque, pour toute autre raison, la possibilité d'un accord pour la publication d'une Norme internationale peut être envisagée pour l'avenir mais pas dans l'immédiat;



— type 3: lorsque le comité technique mixte a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales (ceci pouvant comprendre des informations sur l'état de la technique par exemple).

Les rapports techniques des types 1 et 2 font l'objet d'un nouvel examen trois ans au plus tard après leur publication afin de décider éventuellement de leur transformation en Normes internationales. Les rapports techniques de type 3 ne doivent pas nécessairement être révisés avant que les données fournies ne soient plus jugées valables ou utiles.

L'attention est appelée sur le fait que certains des éléments du présent Rapport technique peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI TR 14516, qui est un Rapport technique de type 3, a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*, en collaboration avec UIT-T. Le texte identique est publié comme Rec. UIT-T X.842.

## 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, *authentification 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 thrid 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.

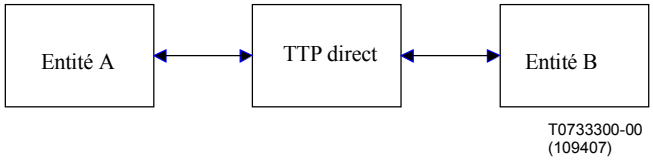


**Figure 1 – Service TTP direct entre entités**

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).

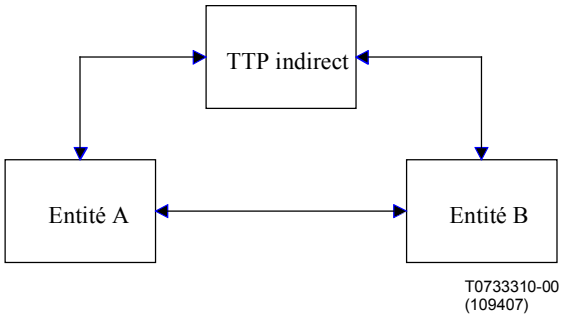


**Figure 2 – Service TTP indirect entre entités**

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).



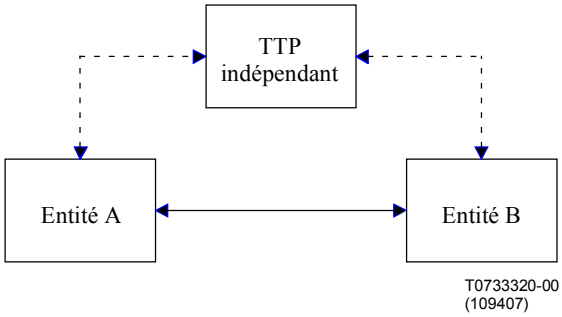


**Figure 3 – Service TTP indépendant entre entités**

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.