NORME INTERNATIONALE

ISO/CEI 15945

Première édition
2002-02-01

Technologies de l'information — Techniques de sécurité — Spécification de services de tiers de confiance TTP pour la prise en charge des applications de signature numérique

Information technology — Security techniques — Specification of TTP services to support the application of digital signatures

Numéro de référence
ISO/CEI 15945:2002(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.ch
Web www.iso.ch

Imprimé en Suisse

TABLE DES MATIÈRES

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.

L'attention est appelée sur le fait que certains des éléments de la présente Norme internationale 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 15945 a été élaborée 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 l'UIT-T. Le texte identique est publié en tant que Rec. UIT-T X.843.

Les annexes A à C de la présente Norme internationale sont données uniquement à titre d'information.

Introduction

Actuellement le développement des technologies de l'information ainsi que celui de l'infrastructure mondiale de communication ouvrent la possibilité d'implémenter le commerce électronique dans des dimensions économiques appropriées. Les signatures numériques constituent une technique importante pour ajouter de la sécurité à ces applications commerciales et à d'autres champs d'application qui ont besoin de transactions électroniques légalement efficaces.

Les signatures numériques conviennent pour assurer l'intégrité des données et l'authentification des participants aux transactions. Elles peuvent constituer une analogie avec la signature manuscrite pour les commandes, offres et contrats numériques. La caractéristique la plus importante des signatures numériques dans ce contexte est qu'une personne ayant signé un document ne peut pas par la suite le nier. Cette caractéristique est appelée "non-répudiation de création" d'un document.

Dans de nombreux pays et dans le contexte international, la législation concernant les signatures numériques est mise en avant dans le but de prendre en charge le développement du commerce électronique et d'autres champs d'application qui ont besoin de transactions électroniques légalement efficaces.

Il existe un certain nombre de normes qui spécifient les signatures numériques ainsi que leur utilisation pour différents besoins tels que la non-répudiation ou l'authentification. Un certain nombre d'applications commerciales ainsi que des services d'offres TTP liés aux signatures numériques sont implémentés ou prévus. L'interopérabilité de ces tiers TTP entre eux et avec les applications commerciales est nécessaire pour une utilisation mondiale économiquement et légalement efficace des signatures numériques.

L'objectif de la présente Recommandation | Norme internationale est de définir les services nécessaires à la prise en charge des applications de signature numérique pour la non-répudiation de création. Comme l'utilisation des mécanismes pour la non-répudiation de création d'un document suppose l'intégrité du document et l'authenticité du créateur, les services décrits dans la présente Recommandation | Norme internationale peuvent également être combinés afin d'implémenter les services pour l'intégrité et l'authenticité. Ceci est réalisé d'une manière qui favorise l'interopérabilité entre tiers TTP ainsi qu'entre tiers TTP et applications commerciales.

NOTE – Il n'y a aucune raison inhérente que chaque tiers TTP prévoyant la prise en charge des applications de signature numérique doive offrir tous ces services. Il est possible que des tiers TTP offrant des services différents coopèrent pour prendre en charge l'utilisation de signatures numériques. Toutefois, du point de vue des applications commerciales potentielles, la totalité de la gamme des services peut être nécessaire et l'interopérabilité devient encore plus importante dans ce scénario. Il s'agit d'une raison supplémentaire de recueillir l'ensemble de tous ces services dans un document unique.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SPÉCIFICATION DE SERVICES DE TIERS DE CONFIANCE (TTP) POUR LA PRISE EN CHARGE DES APPLICATIONS DE SIGNATURE NUMÉRIQUE

1 Domaine d'application

La présente Recommandation | Norme internationale définit les services TTP nécessaires à la prise en charge des applications de signature numérique aux fins de non-répudiation de création de documents.

La présente Recommandation | Norme internationale définit également les interfaces et protocoles permettant l'interopérabilité entre des entités associées à ces services TTP.

Les définitions de services techniques et de protocoles sont nécessaires pour permettre l'implémentation des services TTP et des applications commerciales associées.

La présente Recommandation | Norme internationale est centrée sur:

– l'implémentation et l'interopérabilité;

– les spécifications de services;

– les prescriptions techniques.

La présente Recommandation | Norme internationale ne décrit pas la gestion des tiers TTP ou d'autres questions organisationnelles, d'exploitation ou personnelles. Ces sujets sont principalement couverts dans la Rec. UIT-T X.842 | ISO/CEI TR 14516, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance*.

NOTE 1 – Puisque l'interopérabilité est le sujet principal de la présente Recommandation | Norme internationale, les restrictions suivantes s'appliquent:

i) ne sont pris en considération dans la présente Recommandation | Norme internationale que les services qui peuvent être fournis par un TTP soit aux entités terminales soit à un autre TTP;

ii) ne sont pris en considération que les services qui peuvent être demandés ou fournis au moyen de messages numériques normalisables;

iii) ne sont spécifiés en détail que les services pour lesquels des messages normalisés acceptables à grande échelle peuvent être adoptés au moment de la publication de la présente Recommandation | Norme internationale.

D'autres services seront spécifiés dans des documents distincts lorsque des messages normalisés acceptables à grande échelle seront disponibles pour eux. La définition des services horodateurs en particulier fera l'objet d'un document séparé.

NOTE 2 – La structure des données et les messages figurant dans la présente Recommandation | Norme internationale seront spécifiés conformément aux documents RFC 2510 et 2511 (pour les services de gestion de certificats) et RFC 2560 (pour les services OCSP). Le format de la demande de certificat permet aussi l'interopérabilité avec le système PKCS # 10. Voir l'Annexe C pour des références aux documents mentionnés dans la présente note.

NOTE 3 – Il existe d'autres tentatives de normalisation des services TTP dans des environnements et des applications spécifiques, comme SET ou EDIFACT. Ils ne s'inscrivent pas dans le cadre de la présente Recommandation | Norme internationale.

NOTE 4 – La présente Recommandation | Norme internationale définit des spécifications techniques pour les services. Ces spécifications ne dépendent pas des politiques, des règlements juridiques particuliers ou des modèles organisationnels (qui pourraient par exemple définir comment sont réparties les tâches et les responsabilités entre les autorités de certification et les autorités d'enregistrement). Evidemment, la politique des TTP offrant les services décrits dans la présente Recommandation | Norme internationale devra spécifier comment les règlements juridiques et les autres aspects susmentionnés seront respectés par le TTP. La politique doit en particulier spécifier comment la validité des signatures et des certificats numériques est déterminée.

2 Références normatives

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

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.501 (1997) | ISO/CEI 9594-2:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles.*
- Recommandation UIT-T X.509 (2000) | 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.520 (1997) | ISO/CEI 9594-6:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés.*
- Recommandation UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un (ASN.1): 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.690 (1997) | ISO/CEI 8825-1:1998, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*
- 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 Autres références

- ISO/CEI 9796-2:1997, *Technologies de l'information – Techniques de sécurité – Schémas de signature numérique rétablissant le message – Partie 2: Mécanismes utilisant une fonction de hachage.*
- ISO/CEI 9796-3:2000, *Technologies de l'information – Techniques de sécurité – Schéma de signature numérique rétablissant le message – Partie 3: Mécanismes basés sur les logarithnmes discrets.*
- ISO/CEI 10118-1:1994, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 1: Généralités.*
- ISO/CEI 10118-2:1994, *Technologies de l'information -Techniques de sécurité – Fonctions de brouillage – Partie 2: Fonctions de brouillage utilisant un algorithme de 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 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 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 14888-1:1998, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 1: Généralités.*
- ISO/CEI 14888-2:1999, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 2: Mécanismes basés sur des identités.*
- ISO/CEI 14888-3:1998, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 3: Mécanismes fondés sur certificat*.
- ISO/CEI 15946-2 (à publier), *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur des courbes elliptiques – Partie 2: Signatures digitales*.

3 Définitions

Le terme suivant est utilisé comme défini dans l'ISO/CEI 11770-1:

gestion de clés

Le terme suivant est utilisé comme défini dans l'ISO/CEI 10181-1:

tiers de confiance (TTP, *trusted third party*)

Les termes ci-après sont utilisés tels que définis dans la Rec. UIT-T X.509 | ISO/CEI 9594-8:

certificat CA
autorité de certification (CA)
certificat de clé publique

NOTE – La dénomination abrégée "certificat" sera également employée dans la présente Recommandation | Norme internationale pour désigner un "certificat de clé publique".

politique de certification
liste d'annulation de certificats (CRL, *certificate revocation list*)
chemin de certification

Les termes suivants sont utilisés tels que définis dans l'ISO/CEI 10118-1:

fonction de hachage, fonction de brouillage
code de hachage; valeur de hachage

Le terme suivant est utilisé comme défini dans l'ISO/CEI 14888-1:

paramètre de domaine

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

3.1 services de gestion de certificats: tous les services nécessaires à la maintenance du cycle de vie des certificats, y compris l'enregistrement, certification, distribution et annulation de certificats.

3.2 service de certification: service de création et d'attribution de certificats assuré par une autorité de certification et décrit dans l'ISO/CEI 9594-8:1995.

3.3 signature numérique: transformation cryptographique d'une unité de donnée qui permet au destinataire de l'unité de donnée de prouver l'origine et l'intégrité de cette unité de donnée, qui protège l'émetteur et le destinateur de l'unité de donnée contre un faux fabriqué par un tiers et qui protège l'émetteur contre un faux fabriqué par le destinataire.

NOTE – Les signatures numériques peuvent être utilisées par des entités finales (voir ci-après) pour des besoins d'authentification, d'intégrité de données et de non-répudiation de création de données. L'utilisation aux fins de non-répudiation de création de données est le plus important de ces besoins de disposer de signatures numériques ayant force légale. La définition ci-dessus provient de l'ISO/CEI 9798-1.

3.4 autorité CA de confiance directe: une autorité CA de confiance directe est une autorité CA dont la clé publique a été obtenue et est en cours de mémorisation par une entité finale, en toute confiance et sécurité, et dont la clé publique est acceptée par cette entité finale dans le contexte d'une ou plusieurs applications.

3.5 clé de CA de confiance directe: une clé de CA de confiance directe est une clé publique d'une autorité CA de confiance directe. Elle a été obtenue et est en cours de mémorisation par une entité finale, en toute confiance et sécurité. Elle sert à vérifier des certificats sans être elle-même vérifiée au moyen d'un certificat créé par une autre autorité.

NOTE – Si, par exemple, les autorités CA de plusieurs organisations se certifient réciproquement les unes les autres (voir l'Annexe A), l'autorité CA de confiance directe pour une entité peut être l'autorité CA de l'organisation à laquelle appartient cette entité. Les autorités CA de confiance directe et les clés de CA de confiance directe peuvent varier d'une entité à l'autre. Une entité peut considérer plusieurs autorités CA comme des autorités CA de confiance directe.

3.6 service d'annuaire: service pour la recherche et la récupération d'informations à partir d'un catalogue d'objets bien définis, qui peut contenir des informations sur les certificats, numéros de téléphone, conditions d'accès, adresses, etc. Un exemple en est un service d'annuaire conforme à la Rec. UIT-T X.500 | ISO/CEI 9594-1.

3.7 service de distribution de clés: service de distribution de clés en toute sécurité à des entités autorisées, fourni par un Centre de distribution de clés et décrit dans l'ISO/CEI 11770-1.

3.8 non-répudiation de création: protection contre un démenti fallacieux par une entité du fait qu'elle a créé le contenu d'un message (c'est-à-dire, du fait qu'elle est responsable du contenu d'un message).

3.9 environnement de sécurité personnelle (PSE, *personal security environment*): stockage local sûr pour la clé privée d'une entité, pour la clé d'une autorité CA de confiance directe et pour d'autres données éventuelles. En fonction de la politique de sécurité appliquée par l'entité ou en fonction des prescriptions du système, il peut s'agir par exemple d'un fichier protégé par chiffrement ou d'un jeton de matériel inviolable.

3.10 service de personnalisation: service de stockage d'informations cryptographiques (spécialement des clés privées) dans un environnement PSE.

NOTE – Les mesures organisationnelles et de sécurité physique destinées à un tel service ne s'inscrivent pas dans le domaine d'application de la présente Recommandation | Norme internationale. Pour les mesures organisationnelles, se reporter à la Rec. UIT-T X.842 | ISO/CEI TR 14516, Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance.

3.11 annuaire de clé publique (PKD, *public key directory*): annuaire contenant un (sous-)ensemble bien défini de certificats de clé publique. Cet annuaire peut contenir des certificats provenant de différentes autorités de certification.

3.12 infrastructure de clé publique (PKI, *public key infrastructure*): système constitué de tiers TTP, avec les services qu'ils fournissent pour la prise en charge de l'application (y compris la création et la validation) de signatures numériques, et des personnes ou composants techniques qui utilisent ces services.

NOTE – Parfois on appelle entités finales les personnes et composants techniques qui participent à une infrastructure PKI en utilisant les services de tiers TTP, mais sans être eux-mêmes des tiers TTP. Un exemple d'équipement technique utilisé par une entité finale est une carte à puce qui peut être utilisée comme mémoire de stockage et/ou dispositif de traitement.

3.13 autorité d'enregistrement (RA, *registration authority*): autorité habilitée et chargée en toute confiance d'exécuter un service d'enregistrement tel que décrit ci-dessous.

3.14 service d'enregistrement: service d'identification d'entités et de leur enregistrement d'une manière qui permet l'attribution sûre de certificats à ces entités.

3.15 service d'horodatage: service attestant de l'existence d'une donnée électronique à un moment précis dans le temps.

NOTE – Les services d'horodatage sont utiles et probablement indispensables pour prendre à charge la validation à long terme de signatures. Ils seront définis dans une norme distincte.

4 Abréviations

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

CA Autorité de certification (*certification authority*)

CRL Liste d'annulation de certificat (*certificate revocation list*)

EE Entité finale (*end entity*)

OCSP Protocole de statut de certificat en ligne (*on-line certificate status protocol*)

PKD Annuaire de clé publique (*public key directory*)

PKI Infrastructure de clé publique (*public key infrastructure*)

PSE Environnement de sécurité personnelle (*personal security environment*)

RA Autorité d'enregistrement (*registration authority*)

TTP Tiers de confiance (*trusted third party*)

5 Classification descriptive des services

Le présent article décrit des services qui peuvent être utilisés dans le contexte de services TTP pour des signatures numériques. Une description de haut niveau de ces services y est donnée, indépendante des formats de données, d'algorithmes, de langages de descriptions, etc.

Une spécification détaillée d'un certain nombre de ces services est fournie dans les articles ci-après.

Il n'est pas nécessaire que chaque tiers TTP prévoyant de prendre en charge l'application de signatures numériques offre la totalité de ces services. Il est possible que plusieurs tiers TTP offrant des services différents collaborent dans la prise en charge de l'utilisation de signatures numériques.

NOTE 1 – Sachant que l'interopérabilité est la question principale de la présente Recommandation | Norme internationale, seuls sont décrits ici les services qui sont offerts par un tiers TTP soit à des entités finales soit à un autre tiers TTP. En outre, seuls sont couverts les services qui peuvent être demandés ou fournis à l'aide de messages numériques normalisables. (Cela n'implique pas cependant que les messages normalisés soient effectivement définis pour tous les services mentionnés dans la présente Recommandation | Norme internationale.)

Les exemples suivants illustrent des services qui **ne sont pas** couverts:

1) enregistrement d'événements liés à la sécurité. Compte tenu de l'infrastructure PKI d'une signature numérique, il s'agit d'un service interne de tiers TTP mais qui n'est pas offert à des entités;

2) services cryptographiques généraux (par exemple service de chiffrement). Les procédés tels que le chiffrement font partie de certains services mais ne sont pas pertinents en tant que service autonome dans le contexte des signatures numériques;

3) archivage ou récupération de clés. Il peut s'agir d'un service interne pour les clés de CA de confiance directe. Ces actions ne sont pas généralement exécutées pour les clés de signatures numériques d'entités finales.

NOTE 2 – Les services d'horodatage seront définis dans un document distinct.

5.1 Services de gestion de certificats

Le présent paragraphe contient une description des services suivants qui font partie du cycle de vie des certificats:

- enregistrement;
- certification de clé publique;
- annulation de certificats;
- mise à jour de certificats;
- mise à jour de clé.

Une spécification détaillée du flux de messages en ligne de ces services (à l'exception de la détermination du statut du certificat) est fournie à l'article 7 et la spécification ASN.1 des structures de données nécessaires à ces messages est fournie à l'article 8. Les spécifications analogues pour la détermination du statut de certification en ligne (voir § 5.1.3.3, deuxième méthode) sont fournies à l'article 9.

Les protocoles d'accès à l'annuaire qui sont utilisés pour rendre publiquement disponibles les certificats et listes CRL ne sont pas spécifiés ici car les spécifications pour ces protocoles existent déjà dans les Rec. UIT-T X.511 | ISO/CEI 9594-3 et Rec. UIT-T X.519 | ISO/CEI 9594-5.

NOTE – D'autres protocoles d'accès à l'annuaire sont LDAP (LDAPv2 1777, 2555 et 2587 des RFC) ou l'accès WEB (RFC 2585).

La Figure 1 ci-après fournit un aperçu général de l'architecture d'une infrastructure PKI avec un certain nombre d'exemples de services.

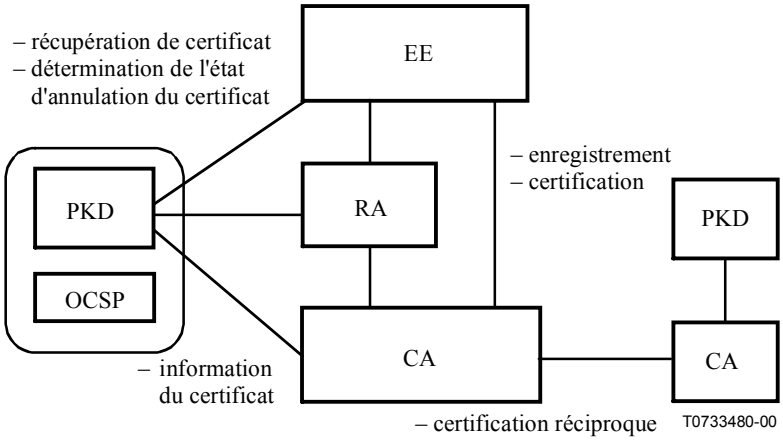

Figure 1 – Aperçu général des services de gestion de certificats

5.1.1 Enregistrement

La véracité d'une infrastructure de clé publique s'appuie sur l'identification et l'enregistrement corrects des entités.

Pour toutes les entités, une autorité RA (qui peut être également une autorité de certification) doit vérifier l'identité des entités finales par des moyens appropriés et doit attribuer un nom unique non ambigu à chaque entité finale à l'intérieur de son domaine. La politique de certification détermine la nature des moyens à utiliser pour effectuer cette identification (par exemple des documents d'identité) et la question de savoir si l'entité finale doit être présente en personne. Une dénomination des noms d'entité finale peut également être nécessaire. Les entités finales qui sont des composants techniques sont enregistrées conformément à la politique de sécurité de l'application, par exemple la gestion de réseau. Il convient que les applications dans lesquelles la différence entre entités finales humaines et non humaines est importante établissent clairement cette distinction dans le certificat. Par exemple, un "nom" pourrait être "dispositif de type X", numéro "Y" situé dans "Z", la distinction pourrait être établie conformément à la politique ou une extension peut indiquer la différence.

Un formulaire d'enregistrement peut être utilisé pour recueillir les données pertinentes, par exemple le nom, l'unité d'entreprise, l'adresse d'entreprise et l'adresse de livraison du matériel de codage.

EXEMPLE: un scénario dans une entreprise peut consister en ce que chaque employé doit être présent en personne au bureau du personnel approprié et montrer sa carte d'identité en cours de validité. Le responsable du personnel en fonction atteste de l'identité et envoie un formulaire d'enregistrement signé à l'autorité de certification.

5.1.2 Certification de clé publique

L'autorité de certification est responsable du processus de certification, du lien d'un nom d'entité ou d'un pseudonyme avec les clés publiques. Un format de certificat est décrit dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

La présente Recommandation | Norme internationale exige que la preuve de la possession de la clé privée correspondant à la clé publique incluse dans le certificat soit apportée au cours du service de certification. En fonction de la politique, une autorité de certification peut garantir d'autres propriétés de la clé publique de l'entité finale, en incluant par exemple l'un ou les deux services décrits aux § 5.3.2 et 5.3.3.

5.1.3 Annulation de certificats

5.1.3.1 Généralités

Un souci majeur avec les certificats de clés publiques est qu'ils peuvent devoir être *annulés* avant le moment prévu de leur expiration à cause de circonstances diverses. L'annulation peut être effectuée par l'autorité CA émettrice ou par une autre autorité en fonction de la politique.

L'annulation est obligatoire si la clé privée a été altérée. D'autres raisons d'annulation peuvent être un changement de nom, la fin d'une période d'embauche, etc.

Il convient que la politique de certification établisse toutes les raisons d'annulation. On peut trouver un certain nombre de ces raisons dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Il convient que la politique définisse qui peut faire les demandes d'annulation et, aussi, si un jeton spécifique peut être utilisé pour identifier des entités autorisées à annuler des certificats tels que les mots de passe d'annulation à usage unique.

5.1.3.2 Méthodes d'annulation

On peut utiliser deux méthodes pour annuler des certificats:

1) Emission d'une liste d'annulation de certificats (CRL)

   Une liste CRL est une liste émise périodiquement et signée par l'autorité de certification et elle identifie tous les certificats qui ont été annulés.

   L'annulation entraîne une saisie immédiate dans la liste CRL, qui inclut également le moment de l'annulation du certificat concerné. En outre, la politique de l'autorité de certification peut exiger de retirer le certificat de l'annuaire des clés publiques PKD.

   NOTE – Selon la politique, il peut être indiqué de conserver le certificat afin de vérifier la validité des signatures apposées avant la date d'annulation (par exemple, lorsque le motif d'annulation n'altère pas la clé).

   Outre la publication périodique, la liste CRL mise à jour peut être publiée immédiatement.

   L'ISO/CEI 11770-1 indique deux horodatages d'annulation différents:

   – le moment de l'altération connue ou suspectée; et
   – le moment auquel l'autorité de certification a été avisée par l'entité de l'altération.

   En fonction de la politique, la saisie du certificat dans la liste CRL peut être effacée lorsque le certificat expire (comparer avec le § 5.1.3.3, Détermination de l'état d'annulation de certificat).

2) Le stockage du statut du certificat dans une base de données interne de confiance de l'autorité de certification et l'offre aux entités d'informations en ligne sur le statut des certificats (comparer avec le § 5.1.3.3. Détermination de l'état d'annulation de certificat).

Ces deux méthodes peuvent être combinées.

Si une clé est altérée, la procédure normale est d'annuler le certificat correspondant, de réinitialiser l'entité finale, de créer une nouvelle paire de clés publique/privée et de certifier la nouvelle clé publique avec les attributs précédents.

En fonction de la politique, un certificat peut:

– être annulé de manière permanente;
– être suspendu. La saisie dans la liste CRL inclut un fanion qui indique l'état "en suspens" ("on hold").

La politique de l'autorité de certification doit spécifier la signification de l'état "en suspens" relativement au niveau de confiance qu'il représente pour une entité et la manière dont il convient qu'une entité traite cette situation. Par exemple, un certificat pourrait être suspendu à la suite d'une demande d'annulation non autorisée. Certaines politiques ne permettent pas du tout l'état "en suspens".

EXEMPLE: une politique peut établir ce qui suit: lorsqu'une vérification est effectuée, elle doit être rejetée tant que le certificat est suspendu. Lorsqu'une preuve est vérifiable à l'aide d'un certificat suspendu, le résultat de la vérification doit être négatif si un résultat est immédiatement nécessaire mais il peut également être interprété comme une validité conditionnelle. Si la suspension est suivie d'une annulation, la preuve devient non valide et la date d'annulation doit être la date du début de la suspension (et non la date de la fin de la suspension).

5.1.3.3 Détermination de l'état d'annulation de certificat

Ce service permet à une entité de déterminer si un certificat est annulé. On peut le faire suivant différentes méthodes qui correspondent aux méthodes d'annulation telles que décrites au § 5.1.3.2:

1) Méthode 1: vérification de l'annuaire PKD et de la liste CRL.
2) Méthode 2: demande en ligne du statut auprès d'un tiers TTP en qui on a confiance pour ce besoin. La réponse du tiers TTP doit être acheminée d'une manière authentique à l'entité.

5.1.3.4 Annulation d'un certificat d'une autorité CA

Un scénario spécial est constitué par l'altération de la clé privée d'une autorité de certification. Si cela se produit:

– le certificat de la clé publique correspondant à la clé altérée de l'autorité CA doit être annulé.

  La confiance en les certificats calculés avec la clé altérée de l'autorité CA n'est plus assurée par la signature de l'autorité CA qui est contenue dans ces certificats. Il est toutefois possible de garantir la validité de ces certificats par d'autres moyens (par exemple, lorsque les certificats sont stockés d'une manière digne de confiance par un TTP qui assure un service OCSP). Dans tous les cas, les entités doivent obtenir un nouveau certificat et une nouvelle clé de l'autorité CA non altérée pour des signatures ultérieures.

En fonction de la politique, les certificats calculés avec la clé altérée sont annulés, ce qui constitue un moyen d'informer les entités finales de la nécessité d'obtenir de nouveaux certificats.

Dans un certain nombre de situations dépendant de la politique de certification et de l'architecture du système, il convient de créer de nouvelles paires de clés destinées aux entités.

Il est important de remarquer que dans un tel scénario, toute signature qui a été émise avant que ne se produise l'altération et qui est sécurisée par des moyens supplémentaires (par exemple horodatée par une autorité d'horodatage dont le certificat est toujours valide) peut être toujours considérée valide en fonction de la politique, alors que toute signature qui a été émise après le moment de l'altération déterminée ou qui n'a pas été sécurisée par des moyens supplémentaires sera considérée non valide;

– si la clé publique correspondant à la clé privée altérée de l'autorité CA est certifiée de manière réciproque avec d'autres autorités CA, un message d'alerte doit être envoyé à ces autorités de certification. Ce message d'alerte leur notifie d'annuler le certificat des autorités de certification qui a été l'objet de certification réciproque.

5.1.4 Mise à jour de certificat

Dans le cas où un certificat expire, il peut être mis à jour en émettant un nouveau certificat pour la clé publique de l'entité qui était déjà contenue dans l'ancien certificat.

On ne doit pas utiliser cette méthode:

– si la paire de clés de l'entité est altérée; ou

– si l'état de cryptographie indique que l'algorithme de clé publique en rapport avec les paramètres de la paire de clés ne peut pas garantir la sécurité des signatures qui ont été créées avec cette paire de clés pour la période de validité du nouveau certificat; ou

– si le nouveau certificat présente des différences substantielles en termes de politique, extensions ou attributs par rapport à l'ancien certificat.

La politique de certification d'une autorité CA peut spécifier qu'une procédure d'enregistrement simplifiée est acceptable pour l'émission d'un nouveau certificat.

EXEMPLE: si l'ancien certificat n'est pas annulé, on peut accepter ce fait comme suffisant pour émettre un nouveau certificat.

La modification d'attributs non critiques dans un certificat pendant sa période de validité, tels que le nom ou l'affiliation (par exemple par un déplacement à un autre département) peut également conduire à la prescription pour une recertification des attributs modifiés, avec les mêmes clés qu'auparavant. Néanmoins, le certificat précédent doit être annulé dans ce cas.

5.1.5 Mise à jour de clés

Une nouvelle paire de clés est créée soit par l'entité elle-même, soit par le tiers TTP et un certificat est émis pour la clé publique de cette nouvelle paire.

Cette méthode doit être choisie dans le cas d'expiration d'un certificat si la mise à jour du certificat n'est pas acceptable pour l'une des raisons fournies au § 5.1.4. Elle peut également être utilisée dans d'autres situations en fonction de la politique de l'autorité de certification.

La politique de certification de l'autorité CA peut spécifier qu'une procédure d'enregistrement simplifiée est acceptable pour l'émission d'un certificat destiné à une clé mise à jour.

5.2 Services de gestion de clés

Des descriptions générales des services de gestion de clés sont fournies dans l'ISO/CEI 11770 (dans toutes les parties).

Le présent paragraphe contient seulement une description des services de gestion de clés qui peuvent être offerts comme faisant partie des services liés au cycle de vie de certificats (comparer avec le § 5.1). La spécification détaillée pour le flux de messages en ligne de ces services dans l'article 7 et la spécification ASN.1 des structures de données dans l'article 8 couvrent les services de gestion de clés tant qu'ils aboutissent à des messages en ligne entre une autorité de certification (CA), une autorité d'enregistrement (RA) ou une entité finale (EE).

5.2.1 Création de clés

Dans le contexte des signatures numériques, des tiers TTP peuvent créer des paires de clés privées/publiques, si les entités ne le font pas elles-mêmes. Bien que ce service puisse être offert par des tiers TTP indépendants, on admet en plus que ce service est fourni par une autorité CA ou une autorité RA en réponse à une demande de certification ou par une entité finale avant une demande de certification.

5.2.2 Distribution de clés

5.2.2.1 Distribution de clés privées

Pour la description du service "distribution de clé", on peut distinguer différents modes de transmission de clé (en ligne ou en mode non connecté) et le composant créateur de clé (tiers TTP ou entité). Dans le cas de la création centralisée de clés, le tiers TTP est responsable de la transmission sécurisée du certificat de clé privée et de clé publique de l'entité. De plus, il doit être garanti qu'une clé privée d'entité est envoyée de manière confidentielle. Il peut en être ainsi par chiffrement de la clé par une clé de transport spéciale (symétrique) connue seulement du tiers TTP et de l'entité correspondante. En variante, la clé privée peut être transmise à l'aide d'outils matériels sécurisés appropriés tels que les cartes à puce par exemple. La transmission de la clé privée n'est pas nécessaire si l'entité est à même de créer sa propre paire de clés asymétrique. Dans ce cas, le tiers TTP doit juste exécuter un certain nombre de vérifications de plausibilité (par exemple si l'entité peut signer un message avec une clé privée correspondant à la clé publique) afin de certifier la clé publique de l'entité et de rendre ce certificat disponible.

5.2.2.2 Distribution de clés publiques

Les clés publiques doivent être disponibles aux entités d'une manière qui garantisse leur authenticité. Dans le cas de clés publiques certifiées, la distribution de clés est réalisée par la distribution du certificat, l'authenticité étant garantie par la signature de l'autorité de certification qui a créé le certificat.

Dans le cas d'une clé de CA de confiance directe, on doit utiliser d'autres moyens de distribution sécurisée. Si des clés privées d'une entité sont distribuées à une entité en utilisant un jeton matériel sécurisé, ce jeton peut également être utilisé pour fournir la clé de l'autorité CA. Dans d'autres cas, un processus supplémentaire est nécessaire. Pour des méthodes à cet effet, consulter l'ISO/CEI 11770-3, § 8.1 Distribution de clés publiques sans tiers de confiance "*Public key distribution without a trusted third party*".

5.2.3 Personnalisation

Le stockage de clés privées et de données supplémentaires peut être obtenu en utilisant un jeton physique. Dans cette situation, la personnalisation d'un jeton doit être prise en charge par l'autorité CA, par l'autorité RA ou par les entités finales. Par exemple, la personnalisation de cartes à puce peut inclure des procédures de mise en place (par exemple la création de système de fichiers), la sélection d'un numéro PIN (Numéro d'identification personnel), au hasard ou un mot de passe, ainsi que la livraison et le stockage de toutes les données pertinentes dans une carte à puce.

5.3 Autres services

5.3.1 Certification réciproque

La certification réciproque est un service offert afin de permettre la vérification de signatures, provenant d'entités finales munies de certificats d'une autorité de certification donnée, par des entités finales munies de certificats d'une autre autorité de certification. Par exemple, une autorité CA1 émet un certificat pour une autorité CA2 appartenant à une autre infrastructure PKI avec l'effet que les entités qui font confiance à CA1 peuvent vérifier les certificats d'entités appartenant à l'autre infrastructure PKI par le biais d'un chemin de certification incluant ce nouveau certificat.

Une spécification détaillée pour le flux de messages en ligne de ce service est fournie dans l'article 7, la spécification ASN.1 des structures de données nécessaires à ces messages étant fournie dans l'article 8.

5.3.2 Validation de paramètres de domaine

La validation de paramètres de domaine est la validation d'un ensemble proposé de paramètres de domaine afin de garantir que chaque paramètre de l'ensemble satisfait à tous les attributs qui sont revendiqués pour ce paramètre.