Groupe de travail Réseau
Request for Comments : 3647
RFC rendue obsolète : 2527
Catégorie : Information

Traduction Claude Brière de L'Isle

S. Chokhani, Orion Security Solutions, Inc.
W. Ford, VeriSign, Inc.
R. Sabett,Cooley Godward LLP
C. Merrill, McCarter & English, LLP
S. Wu, Infoliance, Inc.
novembre 2003

Cadre des pratiques de politique et de certification d'infrastructure de clé publique X.509 pour l'Internet

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document présente un cadre pour aider les rédacteurs de politique de certificat ou de déclaration de pratique de certification pour les participants aux infrastructures de clé publique, comme les autorités de certification, les autorités de politique, et les communautés d'intérêt qui souhaitent s'appuyer sur des certificats. En particulier, le cadre fournit une liste complète des sujets qui devraient (à la discrétion du rédacteur) être couverts dans une politique de certificat ou une déclaration de pratique de certification. Le présent document se substitue à la RFC 2527.

Table des Matières

1. Introduction

1.1 Fondements

En général, un certificat de clé publique (qu'on appellera ici "certificat") lie une clé publique détenue par une entité (comme une personne, une organisation, un compte, appareil ou site) à un ensemble d'informations qui identifient l'entité associée à l'utilisation de la clé privée correspondante. Dans la plupart des cas qui impliquent des certificats d'identité, cette entité est connue comme "sujet" ou "souscripteur" du certificat. Deux exceptions incluent cependant des appareils (auquel cas le souscripteur est usuellement l'individu ou l'organisation qui contrôle l'appareil) et des certificats anonymes (dans lesquels l'identité de l'individu ou organisation n'est pas disponible à partir du certificat lui-même). D'autres types de certificats lient des clés publiques aux attributs d'une entité autres que l'identité de l'entité, comme un rôle, un titre, ou des informations sur la solvabilité.

Un certificat est utilisé par un "utilisateur de certificat" ou "consommateur d'assertion" *(relying party)* qui a besoin d'utiliser, et de s'appuyer sur la pertinence du lien entre la clé publique sujette distribuée via ce certificat et l'identité et/ou les autres attributs du sujet contenus dans ce certificat. Un consommateur d'assertion est fréquemment une entité qui vérifie une signature numérique à partir du sujet du certificat où la signature numérique est associée à une adresse de messagerie électronique, une forme de la Toile, un document électronique, ou autres données. D'autres exemples de consommateur d'assertion peuvent inclure un envoyeur de messages chiffrés au souscripteur, un utilisateur d'un navigateur de la Toile qui s'appuie sur un certificat de serveur durant une session de couche de prise sécurisée (SSL, *secure sockets layer*) et une entité qui fait fonctionner un serveur qui contrôle l'accès aux informations en ligne en utilisant des certificats de client comme mécanisme de contrôle d'accès. En résumé, un consommateur d'assertions est une entité qui utilise une clé publique dans un certificat (pour la vérification et/ou le chiffrement de signature). Le degré de confiance que peut accorder le consommateur d'assertion au lien incorporé dans un certificat dépend de plusieurs facteurs. Ces facteurs peuvent inclure les pratiques suivies par l'autorité de certification (CA, *certification authority*) lors de l'authentification du sujet, la politique de fonctionnement de la CA, ses procédures, et les contrôles de sécurité, la portée de la responsabilité du souscripteur (par exemple, pour protéger la clé privée) et la responsabilité déclarée et les termes et conditions de responsabilité de la CA (par exemple, les garanties, les déclinatoires de garanties, et les limitations de responsabilité).

Un certificat X.509 version 3 peut contenir un champ déclarant que une ou plusieurs politiques de certificat spécifiques s'appliquent à ce certificat [ISO1]. Conformément à X.509, une politique de certificat (CP, *certificate policy*) est "un ensemble désigné de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou classe d'applications avec des exigences communes de sécurité". Une CP peut être utilisée par un consommateur d'assertions pour l'aider à décider si un certificat, et le lien qu'il contient, sont suffisamment de confiance et par ailleurs appropriés pour une application particulière. Le concept de CP est un rejeton du concept de déclaration de politique développé par la messagerie Internet à confidentialité améliorée de la [RFC1422] et développé dans [BAU1]. Les aspects juridiques et de responsabilité présentés au paragraphe 4.9 sont le résultat d'un effort de collaboration entre le groupe de travail PKIX de l'IETF et les membres de l'association américaine des avocats (ABA, *American Bar Association*) qui ont travaillé sur l'acceptation juridique de la signature numérique et le rôle de PKI dans cette acceptation.

Une description plus détaillée des pratiques d'une CA pour la production et la gestion sous ses divers aspects des certificats peut être contenue dans une déclaration de pratique de certification (CPS, *certification practice statement*) publiée ou référencée par la CA. Selon les lignes directrices sur les signatures numériques du comité d'information sur la sécurité de l'association américaine des avocats (qu'on abrègera dans la suite de ce document par "DSG") (voir la note (1) à la Section 10) et les lignes directrices d'évaluation de PKI du comité pour la sécurité de l'information (ci-après appelées "PAG") (2), "une CPS est une déclaration des pratiques qu'emploie une autorité de certification pour produire des certificats" [ABA1], [ABA2]. En général, les CPS décrivent aussi les pratiques en rapport avec tous les services du cycle de vie des certificats (par exemple, la production, la gestion, la révocation, et le renouvellement ou le changement des clés) et les CPS donnent des détails concernant les autres questions d'affaires, juridiques et techniques. Les termes contenus dans une CP ou CPS peuvent être ou non contraignants pour les participants à une PKI comme un contrat. Une CP ou CPS peut elle-même prétendre être un contrat. Plus généralement, cependant, un accord peut incorporer une CP ou CPS par référence et donc tenter de lier les parties à l'accord à tout ou partie de ses termes. Par exemple, certaines PKI peuvent utiliser une CP ou (plus couramment) une CPS qui est incorporée par référence dans l'accord entre un souscripteur et une CA ou RA (appelé "un accord de souscripteur") ou dans l'accord entre un consommateur d'assertion et une CA (appelé un "accord de consommateur d'assertion" (RPA, *relying party agreement*)). Dans d'autres cas, cependant, une CP ou CPS n'a pas de signification contractuelle du tout. Une PKI peut destiner ces CP et CPS à être strictement des documents pour information ou pour divulgation.

1.2 Objet

Le présent document a deux objets. D'abord, il vise à expliquer les concepts de CP et de CPS, décrire les différences entre ces deux concepts, et leurs relations avec les accords de souscripteur et de consommateur d'assertions. Ensuite, le présent document vise à présenter un cadre pour aider les rédacteurs et les utilisateurs de politiques de certificat ou de CPS à préparer et comprendre ces documents. En particulier, le cadre identifie les éléments qui peuvent devoir être pris en compte dans la

formulation d'une CP ou d'un CPS. L'objet n'est pas de définir en soi des politiques de certificat ou de CPS particulières. De plus, ce document ne vise pas à fournir un avis juridique ou des recommandations à l'égard d'exigences ou pratiques particulières qui devraient être contenues dans les CP ou CPS. (De telles recommandations apparaissent cependant dans [ABA2].)

1.3 Domaine d'application

La portée du présent document se limite à la discussion des sujets qui peuvent être couverts dans une CP (comme défini dans X.509) ou une CPS (comme défini dans les DSG et PAG). En particulier, le présent document décrit les types d'informations qui devraient être pris en compte pour les inclure dans une CP ou CPS. Bien que le cadre présenté suppose généralement l'utilisation du format de certificat de X.509 version 3 dans le but de fournir l'assurance de l'identité, il n'est pas prévu que le matériel se restreigne à l'utilisation de ce format de certificat ou de certificats d'identité. Il est plutôt prévu que ce cadre soit adaptable à d'autres formats de certificat et de certificats fournissant des assurances autres que d'identité qui peuvent en venir à être utilisés.

La portée ne s'étend pas à la définition en général des politiques de sécurité (comme la politique de sécurité des organisations, la politique de sécurité des systèmes, ou la politique d'étiquetage des données). De plus, le présent document ne définit par une CP ou CPS spécifique. En présentant un cadre, le présent document devrait être vu et utilisé comme un outil flexible qui présente des sujets qui devraient être considérés comme particulièrement pertinents pour les CP ou CPS, et non comme une formule rigide pour produire des CP ou CPS.

Le présent document suppose que le lecteur est familiarisé avec les concepts généraux des signatures numériques, certificats, et infrastructure de clé publique (PKI), comme utilisées dans X.509, les DSG, et les PAG.

2. Définitions

Le présent document utilise les termes définis suivants :

Données d'activation : Valeurs de données, autres que de clés, qui sont nécessaires pour faire fonctionner des modules cryptographiques et qui doivent être protégés (par exemple, un PIN, un mot de passe, ou une clé partagée détenue manuellement).

Authentification : Processus pour établir que des individus, organisations, ou choses sont qui, ou ce qu'elles, prétendent être. Dans le contexte d'une PKI, l'authentification peut être le processus qui établit qu'un individu ou une organisation qui demande l'accès ou cherche à accéder à quelque chose sous un certain nom est, en fait, le bon individu ou organisation. Cela correspond au second processus impliqué dans l'identification, comme le montre la définition de "identification" ci-dessous. L'authentification peut aussi se référer à un service de sécurité qui fournit l'assurance que des individus, organisations, ou choses sont qui ou ce qu'elles prétendent être ou qu'un message ou d'autres données ont pour origine un individu, organisation, ou appareil spécifique. Donc, il est dit qu'une signature numérique d'un message authentifie l'envoyeur du message.

Certificat de CA : Certificat pour une clé publique de CA produite par une autre CA.

Politique de certificat (CP) : Ensemble désigné de règles qui indiquent l'applicabilité d'un certificat à une communauté et/ou classe d'applications particulière avec des exigences de sécurité communes. Par exemple, une CP particulière pourrait indiquer l'applicabilité d'un type de certificat à l'authentification de parties engageant des transactions d'affaires pour le commerce de biens ou services dans une certaine gamme de prix.

Chemin de certification : Séquence ordonnée de certificats qui, avec la clé publique de l'objet initial dans le chemin, peut être traitée pour obtenir celui de l'objet final dans le chemin.

Déclaration de pratique de certification (CPS, *Certification Practice Statement*) : Déclaration des pratiques qu'une autorité de certification emploie pour produire, gérer, révoquer, renouveler ou changer les clés des certificats.

Résumé de CPS : Sous ensemble des dispositions d'une CPS complète qui est rendue publique par une CA.

Identification : Processus d'établissement de l'identité d'un individu ou d'une organisation, c'est-à-dire, pour montrer qu'un individu ou organisation est un individu ou organisation spécifique. Dans le contexte d'une PKI, identification se réfère à deux processus :

1. établir qu'un certain nom d'un individu ou organisation correspond à la véritable identité de l'individu ou

organisation, et

2. établir qu'un individu ou organisation demandant ou recherchant l'accès à quelque chose sous ce nom est, en fait, l'individu ou organisation désigné. Une personne qui cherche l'identification peut être un demandeur de certificat, un demandeur d'emploi dans une position de confiance au sein d'un participant à une PKI, ou une personne qui cherche à accéder à un réseau ou une application logicielle, comme un administrateur de CA qui cherche à accéder aux systèmes de CA.

Autorité de certification productrice (CA productrice) : Dans le contexte d'un certificat particulier, la CA productrice est la CA qui a produit le certificat (voir aussi Autorité de certification sujette).

Participant : Individu ou organisation qui joue un rôle au sein d'une certaine PKI comme un souscripteur, un consommateur d'assertions, une CA, une RA, une autorité de fabrication de certificats, un fournisseur de service de mémorisation, ou une entité similaire.

Déclaration de divulgation de PKI (PDS, *PKI Disclosure Statement*) : Instrument qui complète une CP ou CPS en divulguant des informations critiques sur les politiques et pratiques d'une CA/PKI. Une PDS est un véhicule pour divulguer et souligner des informations normalement couvertes en détail par les documents de CP et/ou de CPS associés. Par conséquent, une PDS n'est pas destinée à remplacer une CP ou CPS.

Qualificateur de politique : Informations dépendantes de la politique qui peuvent accompagner un identifiant de CP dans un certificat X.509. De telles informations peuvent inclure un pointeur sur l'URL de la CPS applicable ou de l'accord du consommateur d'assertions. Elles peuvent aussi inclure le texte (ou un numéro qui cause l'apparition du texte) qui contient les conditions de l'utilisation du certificat ou d'autres informations juridiques.

Autorité d'enregistrement (RA) : Entité chargé d'une ou plusieurs des fonctions suivantes : l'identification et l'authentification des demandeurs de certificat, l'approbation ou le rejet des demandes de certificat, l'initiation de la révocation ou de la suspension de certificat dans certaines circonstances, le traitement des demandes du souscripteur de révoquer ou suspendre ses certificats, et l'approbation ou le rejet des demandes des souscripteurs de renouveler ou changer les clés de leurs certificats. Cependant les RA ne signent ni ne produisent les certificats (c'est-à-dire, certaines tâches sont déléguées à une RA au nom d'une CA). [Note : le terme de autorité locale d'enregistrement (LRA, *Local Registration Authority*) est parfois utilisé dans d'autres documents pour le même concept.]

Consommateur d'assertions : Receveur d'un certificat qui agit en s'appuyant sur ce certificat et/ou toutes les signatures numériques vérifiées en utilisant ce certificat. Dans le présent document, les termes "utilisateur de certificat" et "consommateur d'assertions" sont utilisés de façon interchangeable.

Accord de consommateur d'assertions (RPA, *Relying party agreement*) : Accord entre une autorité de certification et un consommateur d'assertion qui établit normalement les droits et obligations entre les parties concernant la vérification des signatures numériques ou autres utilisations des certificats.

Ensemble de dispositions : Collection de déclarations de pratiques et/ou de politiques, s'étendant sur une gamme de sujets standard, à utiliser pour exprimer une CP ou CPS employant l'approche décrite dans le présent cadre.

Autorité de certification sujette (CA sujette) : Dans le contexte d'une CA de certificat particulière, la CA sujette est la CA dont la clé publique est certifiée dans le certificat (voir aussi Autorité de certification productrice).

Souscripteur : Sujet d'un certificat à qui est produit un certificat.

Accord de souscripteur : Accord entre une CA et un souscripteur qui établit les droits et obligations des parties en ce qui concerne la production et la gestion des certificats.

Validation : Processus d'identification des demandeurs de certificat. La "validation" est un sous ensemble de "l'identification" et se réfère à l'identification dans le contexte de l'établissement de l'identité des demandeurs de certificat.

3. Concepts

La présente section explique les concepts de CP et de CPS, et décrit leurs relations avec les autres documents de PKI, comme les accords de souscripteur et les accords de consommateur d'assertions. Les autres concepts en rapport sont aussi décrits. Une partie du matériel couvert par cette section et quelques autres sections est spécifique des extensions de politiques de certificat telles que définies dans X.509 version 3. Sauf ces paragraphes, le présent cadre est destiné à s'adapter aux autres formats de certificat qui pourraient venir à être utilisés.

3.1 Politique de certificat

Lorsque une autorité de certification produit un certificat, elle fournit une déclaration à un utilisateur de certificat (c'est-à-dire, un consommateur d'assertions) qu'une clé publique particulière est liée à l'identité et/ou d'autres attributs d'une entité particulière (le sujet du certificat, qui est usuellement aussi le souscripteur). La mesure dans laquelle le consommateur d'assertions devrait s'appuyer sur cette assertion de la CA doit néanmoins être évaluée par le consommateur d'assertions ou l'entité qui contrôle ou coordonne la façon dont les consommateurs d'assertions ou les applications de consommateur d'assertions utilisent les certificats. Des certificats différents sont produits suivant les différentes pratiques et procédures, et peuvent convenir pour des applications et/ou objets différents.

La Recommandation X.509 définit une CP comme "un ensemble désigné de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou classe d'applications qui ont des exigences de sécurité communes" [ISO1]. Un certificat X.509 version 3 peut identifier une CP applicable spécifique, qui peut être utilisée par un consommateur d'assertions pour décider de faire confiance ou non à un certificat, une clé publique associée, ou toute signature numérique vérifiée en utilisant la clé publique pour un objet particulier.

Les CP entrent normalement dans deux grandes catégories. D'abord, certaines CP "indiquent l'applicabilité d'un certificat à une communauté particulière" [ISO1]. Ces CP établissent les exigences pour l'utilisation des certificats et les exigences pour les membres de la communauté. Par exemple, une CP peut se concentrer sur les besoins d'une communauté géographique, comme les exigences de politique d'ETSI pour les CA qui produisent des certificats qualifiés [ETS]. Aussi, une CP de cette sorte peut se concentrer sur les besoins d'une communauté d'un secteur de marché spécifique, comme les services financiers [IDT].

La seconde catégorie de CP typiques "indique l'applicabilité d'un certificat à une . . . classe d'applications qui ont des exigences communes". Ces CP identifient un ensemble d'applications ou usages pour les certificats et disent que ces applications ou usages exigent un certain niveau de sécurité. Elles avancent alors les exigences de PKI qui sont appropriées pour ces applications ou usages. Une CP dans cette catégorie fait souvent des ensembles d'exigences appropriés pour un certain "niveau d'assurance" fourni par les certificats, par rapport aux certificats produits conformément aux CP en rapport. Ces niveaux d'assurance peuvent correspondre aux "classes" ou "types" des certificats.

Par exemple, l'autorité de gestion de la politique de PKI du gouvernement du Canada (GOC PMA, *Policy Management Authority*) a établi huit politiques de certificat dans un seul document [GOC], quatre politiques pour les certificats utilisés pour les signatures numériques et quatre politiques pour les certificats utilisés pour le chiffrement en vue de la protection de la confidentialité. Pour chacune de ces applications, le document établit quatre niveaux d'assurance : rudimentaire, basique, moyen, et élevé. La GOC PMA décrit un certain type de signatures numériques et d'usages de confidentialité dans le document, dont chacun a un certain ensemble d'exigences de sécurité, et les a groupés en huit catégories. La GOC PMA a ensuite établi les exigences de PKI pour chaque catégorie, créant par là huit types de certificats, dont chacun fournit les niveaux d'assurance rudimentaire, basique, moyen, ou élevé. La progression des niveaux de rudimentaire à élevé correspond à des exigences de sécurité croissantes et aux niveaux d'assurance croissants correspondants.

Une CP est représentée dans un certificat par un numéro unique appelé un "Identifiant d'objet" (OID). Cet OID, ou au moins un "arc", peut être enregistré. Un "arc" est le début de la séquence numérique d'un OID et est alloué à une organisation particulière. Le processus d'enregistrement suit les procédures spécifiées dans les normes de l'ISO/CEI et de l'UIT. La partie qui enregistre l'OID ou l'arc peut aussi publier le texte de la CP, pour qu'il soit examiné par les consommateurs d'assertions. Comme un certificat va normalement déclarer une seule CP ou, éventuellement être produit en cohérence avec un petit nombre de politiques différentes. Une telle déclaration apparaît dans l'extension de politique de certificat d'un certificat X.509 version 3. Lorsque une CA place plusieurs CP dans l'extension de politiques de certificat d'un certificat, la CA affirme que le certificat est approprié pour être utilisé conformément à toutes les CP énumérées.

Les CP constituent aussi une base pour un audit, une accréditation, ou autre évaluation d'une CA. Chaque CA peut être évaluée par rapport à une ou plusieurs politiques de certificat ou CPS dont elle reconnaît la mise en œuvre. Lorsque une CA produit un certificat de CA pour une autre CA, la CA productrice doit évaluer l'ensemble des politiques de certificat pour lesquelles elle estime la CA sujette comme de confiance (une telle évaluation peut se fonder sur une évaluation par rapport aux politiques de certificat impliquées). L'ensemble des politiques de certificat évaluées est alors indiqué par la CA productrice dans le certificat de CA. La logique de traitement du chemin de certification X.509 emploie ces indications de CP dans son modèle de confiance bien défini.

3.2 Exemples de politique de certificats

À titre d'exemple, supposons que l'association internationale du transport aérien (IATA) entreprenne de définir des politiques de certificat à utiliser dans toute l'industrie aéronautique, dans une PKI gérée par l'IATA en combinaison avec des PKI gérées par les compagnies aériennes individuelles. Deux CP pourraient être définies : la CP générique de l'IATA, et la CP de nature

commerciale de l'IATA.

La CP générique de l'IATA pourrait être utilisée par les personnels de l'industrie pour protéger les informations de routine (par exemple, la messagerie électronique sans importance) et pour authentifier les connexions entre les navigateurs de la Toile mondiale et les serveurs destinés à la restitution d'informations générales. Les paires de clés peuvent être générées, mémorisées, et gérées en utilisant des systèmes peu coûteux à base de logiciels, comme les navigateurs commerciaux. Sous cette politique, un certificat peut être automatiquement produit pour quiconque figure comme employé dans le répertoire des entreprises de l'IATA ou comme membre d'une compagnie aérienne qui soumet un formulaire de demande de certificat signée à un administrateur de réseau dans son organisation.

La CP commerciale de l'IATA pourrait être utilisée pour protéger les transactions financières ou pour lier les échanges contractuels entre les compagnies aériennes. Sous cette politique, l'IATA pourrait demander que ces paires de clés certifiées soient générées et mémorisées dans des jetons cryptographiques matériels approuvés. Les certificats et les jetons pourraient être fournis aux employés des compagnies aériennes avec l'autorité pour engager de grosses dépenses. Ces individus autorisés pourraient alors être obligés d'être eux-mêmes présents au bureau de sécurité de l'entreprise, de montrer un insigne d'identification valide, et de signer un accord de souscription exigeant d'eux qu'ils protègent le jeton et ne l'utilisent que pour des fins autorisées, comme condition pour produire un jeton et un certificat.

3.3 Champs de certificat X.509

Les champs d'extension suivants d'un certificat X.509 sont utilisés pour prendre en charge les CP :
* extension de politiques de certificat ;
* extension de transposition de politique ;
* extension de contraintes de politique.

3.3.1 Extension de politiques de certificat

Un champ Politiques de certificat fait la liste des CP que l'autorité de certification déclare applicables. En utilisant l'exemple des politiques de niveau commercial et d'objet général de l'IATA définies au paragraphe 3.2, les certificats fournis aux employés réguliers de compagnie aérienne contiendraient l'identifiant d'objet pour la politique d'objet général. Les certificats fournis aux employés avec autorité pour les grosses dépenses contiendraient les identifiants d'objet à la fois pour la politique d'objet général et la politique de niveau commercial. L'inclusion des deux identifiants d'objet dans les certificats signifie qu'ils seraient appropriés aussi bien pour les politiques d'objet général que pour les politiques de niveau commercial. Le champ Politique de certificat peut aussi porter facultativement des valeurs qualifiantes pour chaque politique identifiée ; l'utilisation de qualificatifs est exposée au paragraphe 3.4.

Lors du traitement d'un chemin de certification, une CP qui est acceptable pour l'application de consommateur d'assertions doit être présente dans chaque certificat du chemin, c'est-à-dire, dans les certificats de CA aussi bien que dans les certificats d'entité d'extrémité.

Si le champ Politique de certificat est marqué comme critique, il sert au même objet que décrit ci-dessus mais a aussi un rôle supplémentaire. Précisément, il indique que l'utilisation du certificat est réservée à une des politiques identifiées, c'est-à-dire, l'autorité de certification déclare que le certificat ne doit être utilisé que conformément aux dispositions d'au moins une des CP énumérées. Ce champ est destiné à protéger l'autorité de certification contre des réclamations pour des dommages formulées par un consommateur d'assertions qui a utilisé le certificat dans un but inapproprié ou d'une manière inappropriée, comme stipulé dans la CP applicable.

Par exemple, le service des Impôts pourrait fournir des certificats aux contribuables pour protéger les formulaires de déclaration. Le service des impôts comprend et peut s'accommoder des risques découlant de la production erronée de mauvais certificats, par exemple, à un imposteur. Supposons cependant que quelqu'un ait utilisé un certificat de contribution du service des impôts comme base pour chiffrer des secrets commerciaux brevetés d'une valeur de plusieurs millions d'euros, qui tombent ensuite dans de mauvaises mains à cause d'une attaque de cryptanalyse par un attaquant qui est capable de déchiffrer le message. Le service des impôts peut vouloir se défendre contre les réclamations en dommages et intérêts dans une telle circonstance en pointant la criticité de l'extension de politiques de certificat pour montrer que le souscripteur et consommateur d'assertions a fait un mauvais usage du certificat. L'extension de politique de certificat marquée comme critique est destinée à atténuer le risque pour la CA dans de telles situations.

3.3.2 Extension de transpositions de politique

L'extension de transpositions de politique ne peut être utilisée que dans les certificats de CA. Ce champ permet à une autorité de certification d'indiquer que certaines politiques dans son propre domaine peuvent être considérées comme équivalentes à

certaines autres politiques dans le domaine de l'autorité de certification sujette.

Par exemple, supposons qu'afin de faciliter l'interopérabilité, la Corporation ACE établisse un accord avec la Corporation ABC pour faire une certification croisée des clés publiques de leurs autorités de certification respectives afin de sécuriser mutuellement leurs échanges commerciaux respectifs. Supposons de plus que les deux compagnies aient des politiques préexistantes de protection des transactions financières appelées respectivement ace-e-commerce et abc-e-commerce. On peut voir que générer simplement des certificats croisés entre les deux domaines ne va pas assurer l'interopérabilité nécessaire, car les applications des deux compagnies sont configurée avec, et emploient, des certificats remplis avec leurs politiques de certificat respectives. Une solution possible est de reconfigurer toutes les applications financières pour exiger l'une et l'autre politique et pour produire à nouveau tous les certificats avec les deux politiques qui apparaîtraient dans leurs extensions de politiques de certificat. Une autre solution, qui peut être plus aisée à administrer, utilise le champ Transposition de politique. Si ce champ est inclus dans un certificat croisé pour l'autorité de certification de la corporation ABC produit par l'autorité de certification de la corporation ACE, il peut fournir une déclaration que la politique de protection de transaction financière de ABC (c'est-à-dire, abc-e-commerce) peut être considérée comme équivalente à celle de la corporation ACE (c'est-à-dire, ace-e-commerce). Avec une telle déclaration incluse dans le certificat croisé produit à ABC, les applications de consommateur d'assertions dans le domaine de ACE qui exigent la présence de l'identifiant d'objet pour la CP ace-e-commerce peuvent aussi accepter, traiter, et s'appuyer sur les certificats produits au sein du domaine ABC qui contiennent l'identifiant d'objet pour la CP abc-e-commerce.

3.3.3 Extension de contraintes de politique

L'extension Contraintes de politique prend en charge deux caractéristiques facultatives. La première est la capacité pour une autorité de certification d'exiger que des indications explicites de CP soient présentes dans tous les certificats suivants dans un chemin de certification. Les certificats au début d'un chemin de certification peuvent être considérés par un consommateur d'assertions comme faisant partie d'un domaine de confiance, c'est-à-dire, les autorités de certification sont de confiance pour tous les sujets, de sorte qu'aucune CP particulière n'est nécessaire dans les extensions de politiques de certificat. De tels certificats n'ont pas besoin de contenir des indications explicites de CP. Cependant, lorsque une autorité de certification dans le domaine de confiance certifie en dehors du domaine, elle peut activer l'exigence qu'un identifiant d'objet d'une CP spécifique apparaisse dans les certificats suivants dans le chemin de certification.

L'autre caractéristique facultative du champ Contraintes de politique est la capacité d'une autorité de certification de désactiver la transposition de politique par les autorités de certification suivantes dans un chemin de certification. Il peut être prudent de désactiver la transposition de politique lorsque on certifie en dehors du domaine. Cela peut aider à contrôler les risques dus à la confiance transitive, par exemple, un domaine A fait confiance au domaine B, le domaine B fait confiance au domaine C, mais le domaine A ne veut pas être forcé de faire confiance au domaine C.

3.3.4 Qualificatifs de politique

Le champ d'extension Politique de certificat a une disposition pour porter, avec chaque identifiant de CP, des informations supplémentaires dépendantes de la politique sur un champ qualifiant. La Recommandation X.509 ne rend pas obligatoire l'objet pour lequel ce champ est à utiliser, ni ne prescrit la syntaxe de ce champ. Les types de qualificatifs de politique peuvent être enregistrés par toute organisation.

Les types de qualificatifs de politique suivants sont définis dans PKIX [RFC3280] :

(a) Le qualificatif Pointeur de CPS contient un pointeur sur une CPS, résumé de CPS, RPA, ou PDS publié par la CA. Le pointeur est sous la forme d'un identifiant de ressource universel (URI).

(b) Le qualificatif Notice d'utilisateur contient une chaîne de texte qui est à afficher aux souscripteurs et consommateurs d'assertions avant l'utilisation du certificat. La chaîne de texte peut être une chaîne IA5 ou BMP – un sous ensemble du jeu de caractères codés sur plusieurs octets de ISO 100646-1. Une CA peut invoquer une procédure qui exige que le consommateur d'assertions reconnaisse que les termes et conditions applicables ont été divulgués et/ou acceptés.

Les qualificateurs de politique peuvent être utilisés pour prendre en charge la définition de CP génériques, ou paramétrées. Pourvu que la CP de base en dispose ainsi, les types de qualificateurs de politique peuvent être définis pour porter, certificat par certificat, des détails supplémentaires spécifiques de la politique qui rentrent dans la définition générique.

3.4 Déclaration de pratiques de certification

Le terme de déclaration des pratiques de certification (CPS, *certification practice statement*) est défini par les DSG et PAG comme "une déclaration des pratiques qu'emploie une autorité de certification pour produire les certificats" [ABA1], [ABA2]. Comme on l'a indiqué précédemment, une CPS établit les pratiques concernant le cycle de vie des services en plus de la production, comme la gestion du certificat (incluant la publication et l'archivage) la révocation, et le renouvellement ou

changement de clés. Dans les DSG, l'ABA étend cette définition par le commentaire suivant :
"Une déclaration de pratique de certification peut prendre la forme d'une déclaration par l'autorité de certification des détails de son système de confiance et des pratiques qu'elle emploie dans son fonctionnement et à l'appui de la production d'un certificat . . . ." Cette forme de CPS est du type le plus courant, et peut varier dans sa longueur et son niveau de détail.

Certaines PKI peuvent n'avoir pas besoin de créer une déclaration précise et détaillée de leurs pratiques. Par exemple, la CA peut elle-même être le consommateur d'assertions et aura déjà pleine connaissance de la nature et du niveau de confiance de ses services. Dans d'autres cas, une PKI peut fournir des certificats qui ne procurent qu'un très faible niveau d'assurance et où les applications sécurisées ne font peser que des risques marginaux en cas de compromission. Dans ces cas, une organisation qui établit une PKI peut ne pas vouloir écrire ou avoir des CPS, les CA utilisent un accord de souscription, un accord de consommateur d'assertions, ou un accord combinant les termes de souscripteur et de consommateur d'assertions, selon le rôle des différents participants à la PKI. Dans une telle PKI, cet accord peut servir de seule "déclaration de pratiques" utilisée par une ou plusieurs CA dans cette PKI. Par conséquent, cet accord peut aussi être considéré comme une CPS et peut être intitulé ou sous-titré ainsi.

De même, comme une CPS détaillée peut contenir des détails sensibles sur son système, une CA peut choisir de ne pas publier sa CPS entière. Elle peut à la place opter pour la publication d'un résumé de CPS (ou CPS résumée). La CPS résumée va contenir seulement les dispositions de la CPS que la CA considère pertinentes pour les participants à la PKI (comme les responsabilités des parties ou les étapes du cycle de vie du certificat). Une CPS résumée ne va cependant pas contenir les dispositions sensibles de la CPS complète qui pourraient fournir à un attaquant des informations utiles sur le fonctionnement de la CA. Tout au long du présent document, l'utilisation de "CPS" inclut à la fois la CPS détaillée et la CPS résumée (sauf mention contraire).

Les CPS ne constituent pas automatiquement des contrats et ne lient pas automatiquement les participants à la PKI comme le ferait un contrat. Lorsque un document sert le double objet d'être un accord de souscripteur ou consommateur d'assertions et une CPS, le document est destiné à être un contrat et constitue un lien contractuel dans la mesure ou un accord de souscripteur ou de consommateur d'assertions va ordinairement être considéré comme tel. La plupart des CPS, cependant, ne servent pas ce double objet. Donc, dans la plupart des cas, les termes d'une CPS n'ont un effet obligatoire comme les termes d'un contrat que si un document distinct crée une relation contractuelle entre les parties et que le document incorpore par référence tout ou partie de la CPS. De plus, si une PKI particulière emploie une CPS résumée (par opposition à la CPS entière) la CPS résumée pourrait être incorporée dans tout accord applicable de souscripteur ou consommateur d'assertions.

À l'avenir, la jurisprudence ou des dispositions réglementaires applicables pourraient déclarer qu'un certificat est par lui-même un document capable de créer une relation contractuelle, dans la mesure où ses mécanismes conçus pour incorporation par référence (comme l'extension Politiques de certificat et ses qualificatifs) indiquent que les termes de son utilisation apparaissent dans certains documents. En même temps,certains accords de souscripteur et consommateur d'assertions peuvent cependant incorporer une CPS par référence et donc rendre ses termes liants pour les parties à de tels accords.

3.5 Relations entre politique de certificat et déclaration de pratiques de certification

La CP et la CPS visent le même ensemble d'objets qui sont l'intérêt du consommateur d'assertions en termes de degré de confiance qu'on peut accorder à un certificat de clé publique et à son objet. Leur principale différence est le point sur lequel se concentrent leurs dispositions. Une CP met en avant les exigences et les normes imposées par la PKI à l'égard des divers sujets. En d'autres termes, l'objet de la CP est d'établir ce que les participants doivent faire. Une CPS, à sa différence, déclare comment une CA et les autres participants dans un certain domaine mettent en œuvre les procédures et les contrôles pour satisfaire les exigences déclarées dans la CP. En d'autres termes, l'objet de la CPS est de divulguer comment les participants effectuent leurs fonctions et mettent en œuvre les contrôles.

Des différences supplémentaires entre une CP et une CPS se rapportent à la portée de la couverture des deux sortes de documents. Comme une CP est une déclaration d'exigences, son meilleur usage est celui d'un véhicule pour communiquer le minimum de lignes directrices de fonctionnement qui doit être respecté par les PKI qui interopèrent. Donc, une CP s'applique généralement à plusieurs CA, plusieurs organisations, ou plusieurs domaines. À l'opposé, une CPS ne s'applique qu'à une seule CA ou une seule organisation et n'est généralement pas un véhicule pour faciliter l'interopération.

Une CA avec une seule CPS peut prendre en charge plusieurs CP (utilisées pour des applications d'objet différentes et/ou par des communautés de consommateur d'assertions différentes). Aussi, plusieurs CA, avec des CPS non identiques, peuvent prendre en charge la même CP.

Par exemple, le gouvernement fédéral *(américain)* pourrait définir une CP à l'échelle des services de l'État pour traiter des informations confidentielles de ressources humaines. La CP aura une déclaration large des exigences générales pour les participants au sein de la PKI gouvernementale, et une indication des types d'applications pour lesquelles convient son

utilisation. Chaque département ministériel ou agence qui souhaite faire fonctionner une autorité de certification dans cette PKI peut être obligée d'écrire sa propre déclaration de pratiques de certification pour prendre en charge cette CP en expliquant comment elle satisfait aux exigences de la CP. En même temps, la CPS d'un département ou agence peut prendre en charge d'autres politiques de certificat.

Une différence supplémentaire entre une CP et une CPS concerne le niveau de détail des dispositions de chacune. Bien que le niveau de détail puisse varier parmi les CPS, une CPS va généralement être plus détaillée qu'une CP. Une CPS fournit une description détaillée des procédures et contrôles en place pour satisfaire les exigences de la CP, tandis qu'une CP est plus générale.

Les principales différences entre CP et CPS peuvent donc être résumées comme suit :
(a) Une PKI utilise une CP pour établir les exigences qui déclarent ce que ses participants doivent faire. Une seule CA ou organisation peut utiliser une CPS pour divulguer comment elle satisfait les exigences d'une CP ou comment elle met en œuvre ses pratiques et contrôles.
(b) Une CP facilite l'interopération par la certification croisée, la certification unilatérale, ou par d'autres moyens. Donc, elle est destinée à couvrir plusieurs CA. À l'opposé, une CPS est une déclaration d'une seule CA ou organisation. Son objet n'est pas de faciliter l'interopération (parce c'est la fonction d'une CP).
(c) Une CPS est généralement plus détaillée qu'une CP et spécifie comment la CA satisfait aux exigences spécifiées dans une ou plusieurs CP sous lesquelles elle produit des certificats.

En plus de remplir les extensions de politique de certificat avec l'identifiant d'objet de CP applicable, une autorité de certification peut inclure, dans les certificats qu'elle produit, une référence à sa déclaration de pratiques de certification. Une façon standard de faire cela, en utilisant un qualificatif de CP, est décrite au paragraphe 3.4.

3.6 Relations entre CP, CPS, accords et autres documents

Les CP et CPS jouent un rôle central dans la documentation des exigences et pratiques d'une PKI. Néanmoins, elles ne sont pas les seuls documents pertinents pour une PKI. Par exemple, les accords de souscripteur et de consommateur d'assertions jouent un rôle critique en allouant des responsabilités aux souscripteurs et aux consommateurs d'assertions en ce qui concerne l'utilisation des certificats et des paires de clés. Elles établissent les termes et conditions sous lesquelles les certificats sont produits, gérés, et utilisés. Le terme "accord de souscripteur" est défini par les PAG comme "un accord entre une CA et un souscripteur, qui établit les droits et obligations des parties en ce qui concerne la production et la gestion des certificats" [ABA2]. Les PAG définissent un accord de consommateur d'assertions comme "un accord entre une autorité de certification et un consommateur d'assertions qui établit normalement les droits et obligations entre ces parties concernant la vérification des signatures numériques ou d'autres utilisations des certificats" [ABA2].

Comme mentionné au paragraphe 3.5, un accord de souscripteur, un accord de consommateur d'assertions, ou un accord qui combine les termes de souscripteur et de consommateur d'assertions peut aussi servir de CPS. Dans d'autres PKI, cependant, un accord de souscripteur ou un accord de consommateur d'assertions peut incorporer par référence certains des termes, ou tous, d'une CP ou d'une CPS. D'autres PKI peuvent encore emprunter d'une CP et/ou CPS les termes qui sont applicables à un souscripteur et placer de tels termes dans un accord de souscripteur autonome, sans incorporer par référence de CP ou CPS. Elles peuvent utiliser la même méthode pour emprunter les termes d'un consommateur d'assertions à une CP et/ou CPS et placer de tels termes dans un accord de consommateur d'assertions autonome. Créer de tels accords autonomes présente l'avantage de créer des documents dont la lecture est plus facile pour les consommateurs. Dans certains cas, les souscripteurs ou consommateurs d'assertions peuvent être réputés être les "consommateurs" sous les lois applicables, qui sont l'objet de certaines protections statutaires ou réglementaires. Dans les systèmes juridiques de pays de droit civil, incorporer par référence une CP ou CPS peut n'être pas efficace pour lier les consommateurs aux termes d'une CP ou CPS incorporée.

Les CP et CPS peuvent être incorporées par référence dans d'autres documents, entre autres :
* les accords d'interopérabilité (incluant les accords entre CA pour la certification croisée, la certification unilatérale, ou d'autres formes d'interopération),
* Les accords commerciaux (dans lesquels un vendeur de PKI accepte de satisfaire aux normes établies dans une CP ou CPS)
* une PDS. Voir [ABA2]

Une PDS sert une fonction similaire à celle d'une CPS résumée. C'est un document relativement court qui ne contient qu'un sous ensemble des détails critiques sur une PKI ou CA. Elle peut différer d'une CPS résumée, cependant, en ce que son objet est d'agir comme résumé des informations sur la nature globale de la PKI, et non de simplement condenser la CPS.

De plus, son objet est de diffuser les informations sur la PKI, et non de protéger les informations sensibles pour la sécurité contenues dans une CPS non publiée, bien qu'une PDS puisse aussi servir cette fonction.

Tout comme les rédacteurs peuvent souhaiter se référer à une CP ou CPS ou l'incorporer par référence dans un accord ou une PDS, une CP ou CPS peut se référer à d'autres documents lors de l'établissement des exigences ou pour en assurer la diffusion. Par exemple, une CP peut établir des exigences sur le contenu des certificats en se référant à un document externe qui établit un profil standard de certificat. Référencer des documents externes permet à une CP ou CPS d'imposer des exigences détaillées ou des révélations détaillées sans avoir à reprendre en long et en large des dispositions d'autres documents dans la CP ou CPS. De plus, référencer un document dans une CP ou CPS est une autre façon utile de faire une séparation entre la révélation d'informations publiques et des informations confidentielles sensibles pour la sécurité (en plus ou comme solution de remplacement de la publication d'une CPS résumée). Par exemple, une PKI peut vouloir publier une CP ou CPS, mais conserver les paramètres de construction de site pour des CA de zones de haute sécurité comme des informations confidentielles. Dans ce cas, la CP ou CPS pourrait faire référence à un manuel ou document externe contenant les paramètres détaillés de construction du site.

Les documents auxquels une PKI peut souhaiter se référer dans une CP ou CPS incluent :
* une politique de sécurité,
* des manuels de formation, de fonctionnement, d'installation, et d'utilisation (qui peuvent contenir des exigences opérationnelles),
* des normes qui s'appliquent à des aspects particuliers de la PKI (comme des normes qui spécifient le niveau de protection offert par des jetons matériels utilisés dans la PKI ou des normes applicables à la construction du site),
* les plans de gestion de clés,
* les guides de ressources humaines et d'emploi (qui peuvent décrire des aspects des pratiques de sécurité du personnel),
* les politiques de messagerie électronique (qui peuvent discuter des responsabilités du souscripteur et du consommateur d'assertions, ainsi que des implications de la gestion de clé, si applicable). Voir [ABA2].

3.7 Ensemble de dispositions

Un ensemble de dispositions est une collection de déclarations de pratiques et/ou politiques, couvrant une gamme de sujets standard à utiliser pour exprimer une CP ou CPS en employant l'approche décrite dans le présent cadre couvrant les sujets mentionnés à la Section 5. Ils sont aussi décrits en détail à la Section 4.

Une CP peut être exprimée comme un seul ensemble de dispositions.

Une CPS peut être exprimée comme un seul ensemble de dispositions dont chaque composant vise les exigences d'une ou plusieurs politiques de certificat, ou autrement, comme une collection organisée d'ensembles de dispositions. Par exemple, une CPS pourrait être exprimée comme combinaison de :
(a) une liste de politiques de certificat prises en charge par la CPS ;
(b) pour chaque CP du (a), un ensemble de dispositions qui contient des déclarations répondant à cette CP en remplissant les détails non stipulés dans cette politique ou expressément laissés à la discrétion de la CA (dans sa CPS) ; de telles déclarations servent à établir comment cette CPS particulière met en œuvre les exigences de la CP particulière ;
(c) un ensemble de dispositions qui contiennent des déclarations concernant les pratiques de certification sur la CA, sans considération de la CP.

Les déclarations fournies en (b) et (c) peuvent augmenter ou préciser les stipulations de la CP applicable, mais généralement ne doivent pas entrer en conflit avec les stipulations d'une telle CP. Dans certains cas, cependant, une autorité de politique peut permettre des exceptions aux exigences d'une CP, parce que certains contrôles compensatoires de la CA sont divulgués dans sa CPS et permettent à la CA de donner des assurances qui sont équivalentes à celles fournies par les CA qui sont en pleine conformité avec la CP.

Le présent cadre présente le contenu d'un ensemble de dispositions, sous forme de neuf composants principaux, comme suit :
1. Introduction
2. Publication et entreposage
3. Identification et authentification
4. Exigences du fonctionnement du cycle de vie d'un certificat
5. Facilités, gestion, et contrôles sur le fonctionnement
6. Contrôles de la sécurité technique
7. Certificat, CRL, et profil OCSP
8. Examen de conformité
9. Autres affaires commerciales et juridiques

Les PKI peuvent utiliser ce cadre simple de neuf composants principaux pour écrire une CP ou CPS simple. De plus, une CA peut utiliser ce même cadre pour écrire un accord de souscripteur, de consommateur d'assertions, ou un accord contenant les termes de souscripteur et de consommateur d'assertions. Si une CA utilise ce cadre simple pour construire un accord, elle peut

utiliser la section 1 comme introduction ou développement, elle peut exposer les responsabilités des parties aux sections 2 à 8, et utiliser la section 9 pour couvrir les questions commerciales et juridiques décrites plus en détail, en utilisant l'ordre du paragraphe 4.9 ci-dessous (comme les représentations et garanties, déclinatoires et limitations de responsabilité). L'ordre des sujets dans ce cadre simple et les questions commerciales et juridiques du paragraphe 4.9 est le même que (ou similaire à) l'ordre des sujets dans un accord normal de logiciel ou autre accord de technologie. Donc, une PKI peut établir un ensemble de documents (avec une CP, une CPS, un accord de souscripteur, et un accord de consommateur d'assertions) ayant tous la même structure et ordre des sujets, facilitant par là les comparaisons et transpositions entre ces documents et avec les documents correspondants d'autres PKI.

Ce cadre simple peut aussi être utile pour des accords autres que des accords de souscripteur et de consommateur d'assertions. Par exemple, une CA qui souhaite externaliser certains services à une RA ou autorité de fabrication de certificats (CMA, *certificate manufacturing authority*) peut trouver utile d'utiliser ce cadre comme liste des vérifications à effectuer pour écrire un accord d'autorité d'enregistrement ou un accord d'externalisation. Similairement, deux CA peuvent souhaiter utiliser ce cadre simple pour rédiger un projet d'accord de certification croisée, de certification unilatérale, ou autre accord d'interopérabilité.

En bref, les principaux composants du cadre simple (spécifié ci-dessus) peuvent satisfaire les besoins des rédacteurs de brefs CP, CPS, accords de souscripteur, et accords de consommateur d'assertions. Néanmoins, ce cadre est extensible, et sa couverture des neuf composants est assez souple pour satisfaire les besoins des rédacteurs de CP et CPS complètes. Précisément, les composants qui apparaissent ci-dessus peuvent être redivisés en sous composants, et un sous composant peut comporter plusieurs éléments. La Section 4 donne une description plus détaillée du contenu des composants ci-dessus et de leurs sous composants. Les rédacteurs de CP et CPS peuvent ajouter des niveaux supplémentaires de sous composants en dessous de ceux décrits à la Section 4 afin de satisfaire aux besoins de la PKI particulière du rédacteur.

4. Contenu d'un ensemble de dispositions

La présente section développe les contenus du cadre simple de dispositions, comme mentionné au paragraphe 3.7. Les sujets identifiés dans cette section sont par conséquent, des candidats à l'inclusion dans une CP ou CPS détaillée.

Bien que de nombreux sujets soient identifiés, il n'est pas nécessaire qu'une CP ou CPS inclue une déclaration concrète de chacun de ces sujets. Une CP ou CPS particulière peut plutôt déclarer "pas de stipulation" pour un composant, sous composant, ou élément sur lequel cette CP ou CPS n'impose pas d'exigence ou ne fait aucune révélation. Dans ce sens, la liste des sujets peut être considérée comme une liste de vérification des sujets à prendre en considération par le rédacteur de CP ou CPS.

Il est recommandé que chaque composant et sous composant soit inclus dans une CP ou CPS, même si il n'y a "aucune stipulation" ; cela va indiquer au lecteur qu'une décision consciente a été prise d'inclure ou exclure une disposition concernant ce sujet. Ce style de rédaction protège contre une omission involontaire d'un sujet, tout en facilitant la comparaison de différentes politiques de certificat ou de CPS, par exemple, lors de décisions de transposition de politique.

Dans une CP, il est possible de laisser certains composants, sous components, et/ou éléments non spécifiés, et de stipuler que les informations requises seront indiquées dans un qualificatif de politique, ou le document sur lequel pointe un qualificatif de politique. De telles CP peuvent être considérées comme des définitions paramétrées. Les ensembles de dispositions devraient faire référence ou définir les types de qualificatifs de politique requis et devraient spécifier toutes les valeurs par défaut applicables.

4.1 Introductions

Ce composant identifie et introduit les ensembles de dispositions, et indique les types d'entités et applications pour lesquelles le document (la CP ou la CPS en cours de rédaction) est ciblé.

4.1.1 Généralités

Ce sous composant donne une introduction générale au document à rédiger. Ce sous composant peut aussi être utilisé pour donner un synopsis de la PKI à laquelle s'applique la CP ou CPS. Par exemple, il peut établir les différents niveaux d'assurance fournis par les certificats dans la PKI. Selon la complexité et la portée de la PKI particulière, une représentation de la PKI par un diagramme pourrait y être utile.

4.1.2 Nom et identification du document

Ce sous composant donne tous les noms applicables ou les autres identifiants, incluant les identifiants d'objet ASN.1, pour le document. Un exemple d'un tel nom de document pourrait être "Politique du Gouvernement fédéral américain pour la messagerie électronique sécurisée".

4.1.3 Participants à la PKI

Ce sous composant décrit l'identité ou les types d'entités qui tiennent les rôles de participants dans une PKI, à savoir :

* Les autorités de certification, c'est-à-dire, les entités qui produisent les certificats. Une CA est la CA productrice par rapport aux certificats qu'elle produit et est la CA sujette par rapport au certificat de CA qui lui est produit. Les CA peuvent être organisées en une hiérarchie dans laquelle la CA d'une organisation produit des certificats aux CA gérées par les organisations subordonnées, comme une branche, une division, ou un département au sein d'une plus grande organisation.
* Les autorités d'enregistrement, c'est-à-dire, les entités qui établissent les procédures d'engagement pour les demandeurs de certificat d'utilisateur final, effectuent l'identification et l'authentification des demandeurs de certificat, initient ou passent les demandes de révocation pour les certificats, et approuvent les demandes de renouvellement ou les certificats de changement de clés au nom d'une CA. Les organisations subordonnées au sein d'une plus grande organisation peuvent agir comme des RA pour la CA qui dessert l'organisation entière, mais les RA peuvent aussi être externes à la CA.
* Les souscripteurs. Des exemples de souscripteurs qui reçoivent des certificats d'une CA incluent des employés d'une organisation qui a sa propre CA, des clients de banque ou de courtier, des organisations qui hébergent des sites de commerce électronique, des organisations qui participent à un échange entre professionnels, et des membres du public qui reçoivent des certificats d'une CA qui produit des certificats au public au sens large.
* Des consommateurs d'assertions. Des exemples de consommateurs d'assertions incluent des employés d'une organisation qui a sa propre CA qui reçoit des courriers électroniques signés numériquement des autres employés, des personnes qui achètent des biens et services sur des sites de commerce électronique, des organisations qui participent à des échanges entre professionnels qui reçoivent des enchères ou des ordres d'autres organisations participantes, et des individus et organisations qui font des affaires avec des souscripteurs qui ont reçu leurs certificats d'une CA qui produit des certificats au public. Les consommateurs d'assertions peuvent être aussi ou non des souscripteurs au sein d'une certaine PKI.
* Les autres participants, comme des autorité de fabrication de certificats, des fournisseurs de service d'entreposage, et d'autres entités qui fournissent des services en rapport avec la PKI.

4.1.4 Utilisation du certificat

Ce sous composant contient :

* une liste ou les types d'applications pour lesquelles conviennent les certificats produits, comme une messagerie électronique, des transactions de vente au détail, des contrats, et un ordre de voyage, et/ou
* une liste ou les types d'applications pour lesquelles l'utilisation des certificats produits est interdite.

Dans le cas d'une CP ou CPS qui décrit différents niveaux d'assurance, ce sous composant peut décrire les applications ou types d'applications qui sont appropriées ou inappropriées pour les différents niveaux d'assurance.

4.1.5 Administration de la politique

Ce sous composant inclut le nom et l'adresse de messagerie de l'organisation qui est responsable du projet, de l'enregistrement, de la maintenance, et de la mise à jour de cette CP ou CPS. Il inclut aussi le nom, l'adresse de messagerie électronique, le numéro de téléphone, et le numéro de télécopie de la personne à contacter. Au lieu de désigner une vraie personne, le document peut désigner un titre ou rôle, un alias, et autres informations de contact générales. Dans certains cas, l'organisation peut déclarer la personne à contacter, seule ou en combinaison avec d'autres, qui est disponible pour répondre aux questions sur le document.

De plus, lorsque une autorité formelle ou informelle de politique est chargée de déterminer si il devrait être permis à une CA de fonctionner au sein d'une PKI ou d'interopérer avec elle, elle peut souhaiter approuver la CPS de la CA comme convenant pour la CP de l'autorité de politique. Si il en est ainsi, ce sous composant peut inclure le nom ou titre, l'adresse de messagerie électronique (ou l'alias), le numéro de téléphone, le numéro de télécopie et les autres informations générales de l'entité en charge de faire une telle détermination. Finalement, dans ce cas, ce sous composant inclut aussi les procédures par lesquelles cette détermination est faite.

4.1.6 Définitions et acronymes

Ce sous composant contient une liste des définitions des termes utilisés dans le document, ainsi qu'une liste des acronymes dans le document et leur signification.

4.2 Responsabilité des publication et des répertoires

Ce composant contient toutes les dispositions applicables en ce qui concerne :

* l'identification de la ou des entités qui gèrent des répertoires au sein de la PKI, comme une CA, une autorité de fabrication de certificat, ou un fournisseur de service de répertoire indépendant ;
* la responsabilité d'un participant à la PKI de publier les informations concernant ses pratiques, les certificats, et l'état actuel de tels certificats, qui peut inclure la responsabilité de rendre la CP ou CPS publiquement disponible en utilisant divers mécanismes et composants d'identification, de sous composants, et éléments de tels documents qui existent mais ne sont pas publiquement disponibles, par exemple, les contrôles de sécurité, les procédures d'accréditation, ou les informations de secrets commerciaux à cause de leur sensibilité ;
* lorsque les informations doivent être publiées et la fréquence de publication ;
* le contrôle d'accès sur les objets d'informations publiés incluant les CP, CPS, certificats, états de certificat, et CRL.

4.3 Identification et authentification

Ce composant décrit les procédures utilisées pour authentifier l'identité et/ou d'autres attributs d'un demandeur de certificat d'utilisateur d'extrémité à une CA ou RA avant la production du certificat. De plus, le composant met en route les procédures d'authentification de l'identité et les critères pour accepter les demandes d'entités qui cherchent à devenir des CA, RA, ou autres entités qui fonctionnent dans, ou interopèrent avec, une PKI. Il décrit aussi comment sont authentifiées les parties qui demandent un changement de clé ou leur révocation. Ce composant traite aussi des pratiques de désignation, incluant la reconnaissance des droits commerciaux sur certains noms.

4.3.1 Dénominations

Ce sous composant inclut les éléments suivants concernant la dénomination et l'identification des souscripteurs :

* les types de noms alloués au sujet, comme les noms distinctifs X.500, les noms de la RFC-822, et les noms X.400 ;
* si les noms doivent avoir ou non une signification ; (3)
* si les souscripteurs peuvent être ou non anonymes ou des pseudonymes, et si ils le peuvent, quels noms sont alloués ou peuvent être utilisés par les souscripteurs anonymes ;
* les règles d'interprétation des diverses formes de noms, comme des normes X.500 et RFC-822 ;
* si les noms doivent être uniques ;
* la reconnaissance, l'authentification, et le rôle des marques commerciales.

4.3.2 Validation initiale d'identité

Ce sous composant contient les éléments suivants pour les procédures d'identification et d'authentification pour l'enregistrement initial de chaque type de sujet (CA, RA, souscripteur, ou autre participant) :

* si et comment le sujet doit prouver la possession de la clé privée correspondante de la clé publique enregistrée, par exemple, une signature numérique dans le message de demande de certificat ; (4)
* les exigences d'identification et d'authentification pour l'identité d'organisation du souscripteur ou participant (CA, RA, souscripteur (dans le cas de certificats produits à des organisations ou appareils contrôlés par une organisation) ou autre participant) par exemple, en consultant la base de données d'un service qui identifie les organisations ou en inspectant les articles d'incorporation d'une organisation ;
* les exigences d'identification et d'authentification pour un souscripteur individuel ou une personne agissant au nom d'un souscripteur d'organisation ou participant (CA, RA, dans le cas de certificats produits à des organisations ou appareils contrôlés par une organisation, le souscripteur, ou autre participant) (5) incluant :
  * le type de documentation et/ou le nombre d'accréditifs d'identification requis ;
  * comment une CA ou RA authentifie l'identité de l'organisation ou individu sur la base de la documentation ou des accréditifs fournis ;
  * si l'individu doit se présenter personnellement à la CA ou RA authentifiante ;
  * comment un individu est authentifié comme personne d'une organisation, comme par référence à des documents d'autorisation dûment signés ou un insigne d'identification d'entreprise.
* la liste des informations de souscripteur qui ne sont pas vérifiées (appelées "informations de souscripteur non vérifiées") durant l'enregistrement initial ;
* la validation de l'autorité implique la détermination qu'une personne a des droits spécifiques, des titres, ou des permissions, incluant la permission d'agir au nom d'une organisation pour obtenir un certificat ;
* dans le cas de demandes par une CA qui souhaite opérer au sein de, ou interopérer avec, une PKI, ce sous composant contient les critères par lesquels une PKI, une CA, ou une autorité de politique détermine si la CA convient ou non pour une telle opération ou interopération. Une telle interopération peut inclure la certification croisée, la certification unilatérale, ou d'autres formes d'interopération.

4.3.3 Identification et authentification pour les demandes de changement de clés

Ce sous composant s'adresse aux éléments suivants pour les procédures d'identification et d'authentification de changement de clé pour chaque type de sujet (CA, RA, souscripteur, et autres participants) :

* les exigences d'identification et d'authentification pour les changements de clé de routine, comme une demande de changement de clé qui contient la nouvelle clé et est signée en utilisant la clé valide en cours ;
* les exigences d'identification et d'authentification pour le changement de clé après une révocation du certificat. Un exemple est l'utilisation du même processus que la validation d'identité initiale.

4.3.4 Identification et authentification pour les demandes de révocation

Ce sous composant décrit les procédures d'identification et d'authentification pour une demande de révocation par chaque type de sujet (CA, RA, souscripteur, et autre participant). Des exemples incluent une demande de révocation signée numériquement avec la clé privée dont la clé publique correspondante a besoin d'être révoquée, et une demande signée numériquement par la RA.

4.4 Exigences pour le fonctionnement du cycle de vie du certificat

Ce composant est utilisé pour spécifier les exigences imposées à la CA productrice, aux CA sujettes, aux RA, aux souscripteurs, ou aux autres participants à l'égard du cycle de vie d'un certificat.

Au sein de chaque sous composant, il faut considérer séparément les CA sujettes, les RA, les souscripteurs, et les autres participants.

4.4.1 Demande de certificat

Ce sous composant est utilisé pour traiter les exigences suivantes concernant la demande de certificat de sujet :

* qui peut soumettre une demande de certificat, comme un sujet de certificat ou la RA ;
* le processus d'engagement utilisé par les sujets pour soumettre les demandes de certificat et les responsabilités qui découlent de ce processus. Un exemple de ce processus est celui où le sujet génère la paire de clés et envoie une demande de certificat à la RA. La RA valide et signe la demande et l'envoie à la CA. Une CA ou RA peut avoir la responsabilité de l'établissement d'un processus d'engagement afin de recevoir les demandes de certificat. De même, les demandeurs de certificat peuvent avoir la responsabilité de fournir des informations précises sur leurs demandes de certificat.

4.4.2 Traitement de demande de certificat

Ce sous composant est utilisé pour décrire la procédure de traitement des demandes de certificat. Par exemple, la CA et RA productrices peuvent effectuer les procédures d'identification et d'authentification pour valider la demande de certificat. Suivant ces étapes, la CA ou RA va approuver ou rejeter la demande de certificat, peut-être selon l'application de certains critères. Finalement ce sous composant établit une limite de temps durant laquelle une CA et/ou RA doit agir sur une demande de certificat et la traiter.

4.4.3 Production de certificat

Ce sous composant est utilisé pour décrire les éléments suivants relatifs à la production d'un certificat :

* les actions effectuées par la CA durant la production du certificat, par exemple une procédure par laquelle la CA valide la signature et l'autorité de la RA et génère un certificat ;
* les mécanismes de notification, si il y en a, utilisés par la CA pour notifier au souscripteur la production du certificat ; par exemple, une procédure sous laquelle la CA envoie par courrier électronique le certificat au souscripteur ou à la RA ou des informations permettant au souscripteur de télécharger le certificat à partir d'un site de la Toile.

4.4.4 Acceptation de certificat

Ce sous composant s'adresse à ce qui suit :

* La conduite d'une demande qui sera réputée constituer l'acceptation du certificat. Une telle conduite peut inclure des étapes affirmatives pour indiquer l'acceptation, des actions qui impliquent l'acceptation, ou un échec à faire des objections au certificat ou à son contenu. Par exemple, l'acceptation peut être réputée survenir si la CA ne reçoit aucune remarque du souscripteur dans un certain délai ; un souscripteur peut envoyer un message signé acceptant le certificat ; ou un

souscripteur peut envoyer un message signé rejetant le certificat et contenant la raison du rejet et identifiant les champs du certificat qui sont incorrects ou incomplets.
* La publication du certificat par la CA. Par exemple, la CA peut envoyer le certificat à un dépôt X.500 ou LDAP.
* La notification de la production d'un certificat par la CA aux autres entités. Par exemple, la CA peut envoyer le certificat à la RA.

4.4.5 Usage de la paire de clés et du certificat

Ce sous composant est utilisé pour décrire les responsabilités en rapport avec l'usage des clés et certificats, incluant :
* Les responsabilités du souscripteur à l'égard de l'utilisation de sa clé privée et de son certificat. Par exemple, il peut être exigé du souscripteur qu'il n'utilise une clé privée et un certificat que pour des applications appropriées comme établi dans la CP et en cohérence avec le contenu applicable du certificat (par exemple, le champ Usage de clé). L'utilisation d'une clé privée et d'un certificat est soumise aux termes de l'accord de souscripteur, l'usage d'une clé privée n'est permis qu'après que le souscripteur a accepté le certificat correspondant, ou le souscripteur doit cesser d'utiliser la clé privée à partir de l'expiration ou la révocation du certificat.
* Les responsabilités du consommateur d'assertions à l'égard de l'utilisation de la clé publique et du certificat du souscripteur. Par exemple, un consommateur d'assertions peut être obligé de ne s'appuyer sur des certificats que pour des applications appropriées selon ce qui est établi dans la CP et en cohérence avec le contenu applicable du certificat (par exemple, le champ Usage de clé) effectuer avec succès des opérations de clé publique comme condition pour s'appuyer sur un certificat, assumer la responsabilité de vérifier l'état d'un certificat en utilisant un des mécanismes exigés ou permis décrits dans la CP/CPS (voir le paragraphe 4.4.9) et accepter les termes de l'accord de consommateur d'assertions applicable comme une condition pour s'appuyer sur le certificat.

4.4.6 Renouvellement de certificat

Ce sous composant est utilisé pour décrire les éléments suivants en rapport avec le renouvellement de certificat. Renouvellement de certificat signifie la production d'un nouveau certificat au souscripteur sans changer la clé publique du souscripteur ou d'un autre ni aucune autre information du certificat :
* les circonstances dans lesquelles le renouvellement de certificat a lieu, comme le moment où la durée de vie du certificat s'est terminée, mais la politique permet que la même paire de clés soit réutilisée ;
* qui peut demander le renouvellement du certificat, par exemple, le souscripteur, la RA, ou la CA peuvent automatiquement renouveler un certificat de souscripteur d'utilisateur final ;
* les procédures de CA ou RA pour traiter les demandes de renouvellement pour produire le nouveau certificat, par exemple, l'utilisation d'un jeton, comme un mot de passe, pour ré-authentifier le souscripteur, ou des procédures qui sont les mêmes que pour la production du certificat initial ;
* la notification du nouveau certificat au souscripteur ;
* la conduite qui constitue une acceptation du certificat ;
* la publication du certificat par la CA ;
* la notification de la production du certificat par la CA aux autres entités.

4.4.7 Changement de clés de certificat

Ce sous composant est utilisé pour décrire les éléments suivants en rapport avec la génération par un souscripteur ou autre participant d'une nouvelle paire de clés et la demande de production d'un nouveau certificat pour la nouvelle clé publique :
* les circonstances dans lesquelles le changement de clés de certificat peut ou doit avoir lieu, comme après la révocation d'un certificat pour des raisons de compromission de clé ou après qu'un certificat soit arrivé à expiration et que la période d'usage de la paire de clés a aussi expiré ;
* qui peut demander un changement des clés de certificat, par exemple, le souscripteur ;
* les procédures de CA ou RA pour traiter les demandes de changement de clés pour produire le nouveau certificat, comme les procédures qui sont les mêmes que celles de la production initiale du certificat ;
* la notification du nouveau certificat au souscripteur ;
* la conduite qui constitue une acceptation du certificat ;
* la publication du certificat par la CA ;
* la notification de la production du certificat par la CA aux autres entités.

4.4.8 Modification de certificat

Ce sous composant est utilisé pour décrire les éléments suivants relatifs à la production d'un nouveau certificat (6) due aux changements des informations du certificat autres que la clé publique du souscripteur :
* les circonstances dans lesquelles la modification de certificat peut avoir lieu, comme un changement de nom, un changement de rôle, une réorganisation résultant en un changement du DN ;

* qui peut demander une modification de certificat, par exemple, les souscripteurs, le personnel des ressources humaines, ou la RA ;
* les procédures de CA ou RA pour traiter les demandes de modification pour produire le nouveau certificat, comme les procédures qui sont les mêmes qu'à la production du certificat initial ;
* la notification du nouveau certificat au souscripteur ;
* la conduite qui constitue une acceptation du certificat ;
* la publication du certificat par la CA ;
* la notification de la production du certificat par la CA aux autres entités.

4.4.9 Révocation et suspension de certificat

Ce sous composant s'adresse à ce qui suit :

* les circonstances dans lesquelles un certificat peut être suspendu et les circonstances dans lesquelles il doit être révoqué, par exemple, dans le cas de fin d'emploi du souscripteur, de perte du jeton cryptographique, ou de suspicion de compromission de la clé privée ;
* qui peut demander la révocation du certificat du participant, par exemple, le souscripteur, RA, ou CA dans le cas d'un certificat de souscripteur d'utilisateur d'extrémité.
* les procédures utilisées pour une demande de révocation de certificat, comme un message signé numériquement de la RA, un message signé numériquement du souscripteur, ou un appel téléphonique de la RA ;
* la période de grâce disponible pour le souscripteur, dans laquelle il doit effectuer une demande de révocation ;
* le délai dans lequel la CA doit traiter la demande de révocation ;
* les mécanismes, si il y en a, qu'un consommateur d'assertions peut ou doit utiliser pour vérifier l'état des certificats sur lesquels il souhaite s'appuyer ;
* si un mécanisme de CRL est utilisé, la fréquence de production ;
* si un mécanisme de CRL est utilisé, la latence maximum entre la génération des CRL et l'envoi des CRL au dépôt (en d'autres termes, le délai maximum de traitement et de communication de l'envoi des CRL au dépôt après la génération de CRL) ;
* la disponibilité en ligne de la vérification de révocation/état, par exemple, OCSP et un site de la Toile auquel peuvent être soumises les recherches sur l'état ;
* les exigences pour les consommateurs d'assertions quand ils effectuent les vérifications en ligne de révocation/état ;
* les autres formes d'annonce de révocation disponibles ;
* toutes variations des stipulations ci-dessus pour lesquelles la suspension ou la révocation est le résultat de la compromission de la clé privée (par opposition à d'autres raisons de suspension ou révocation) ;
* les circonstances dans lesquelles un certificat peut être suspendu ;
* qui peut demander la suspension d'un certificat, par exemple, le souscripteur, le personnel des ressources humaines, un superviseur du souscripteur, ou la RA dans le cas d'un certificat de souscripteur d'utilisateur d'extrémité ;
* les procédures pour demander la suspension du certificat, comme un message signé numériquement du souscripteur ou de la RA, ou un appel téléphonique de la RA ;
* quelle est la durée de suspension permise.

4.4.10 Services d'état de certificat

Ce sous composant s'adresse aux services de vérification d'état du certificat disponibles pour les consommateurs d'assertions, incluant :

* les caractéristiques du fonctionnement des services de vérification de l'état du certificat ;
* la disponibilité de ces services, et toutes les politiques applicables en cas d'indisponibilité ;
* toutes les caractéristiques disponibles de ces services.

4.4.11 Fin d'abonnement

Ce sous composant s'adresse aux procédures utilisées par le souscripteur pour mettre fin à l'abonnement aux services de la CA, incluant :

* la révocation des certificats à la fin de l'abonnement (qui peut différer, selon que la fin de l'abonnement est dû à l'expiration du certificat ou au terme du service).

4.4.12 Mise en dépôt et récupération de clé

Ce sous composant contient les éléments suivants pour identifier les politiques et pratiques qui se rapportent à la mise en dépôt et/ou la récupération de clés privées lorsque des services de mise en dépôt de clé privée sont disponibles (par l'intermédiaire de la CA ou autre tiers de confiance) :

* identification du document qui contient les politiques e t pratiques de mise en dépôt et récupération de clé privée ou une

liste de telles politiques et pratiques ;
* identification du document contenant des politiques et pratiques d'encapsulation et de récupération de clé de session ou une liste de telles politiques et pratiques.

4.5 Contrôles sur la gestion, le fonctionnement et les caractéristiques physiques

Ce composant décrit les contrôles de sécurité non techniques (c'est-à-dire, physiques, procéduraux, et de personnel) utilisés par la CA productrice pour effectuer en toute sécurité les fonctions de génération de clé, d'authentification de sujet, de production du certificat, de révocation du certificat, d'analyse des problèmes, et d'archivage.

Ce composant peut aussi être utilisé pour définir des contrôles de sécurité non techniques sur les dépôts, les CA sujettes, les RA, les souscripteurs, et autres participants. Les contrôles de sécurité non techniques pour les CA sujettes, les RA, les souscripteurs, et autres participants pourraient être les mêmes, similaires, ou très différents.

Ces contrôles de sécurité non techniques sont critiques pour la confiance dans les certificats car le manque de sécurité peut compromettre le fonctionnement de la CA résultant par exemple, en la création de certificats ou de CRL avec des informations erronées ou en compromettant la clé privée de la CA.

Dans chaque sous composant, des considérations séparées vont, en général, devoir être données à chaque type d'entité, qui sont la CA productrices, le dépôt, les CA sujettes, les RA, les souscripteurs, et les autres participants.

4.5.1 Contrôle de la sécurité physique

Dans ce sous composant sont décrits les contrôles physiques de la facilité qui héberge les systèmes d'entité. Les sujets traités peuvent inclure :
* la localisation et la construction des sites, comme les exigences de construction des zones de haute sécurité et l'utilisation de chambres de confinement, de cages, de coffres forts, et de cabinets de sécurité ;
* l'accès physique, c'est-à-dire, les mécanismes de contrôle d'accès d'une zone de la facilité à une autre ou l'accès à des zones de haute sécurité, comme de localiser les opérations de CA dans un local informatique sécurisé surveillé par des gardes ou des alarmes de sécurité et exigeant que les mouvements de zone à zone soient accomplis en utilisant un jeton, un lecteur biométrique, et/ou des listes de contrôle d'accès ;
* une régulation de l'alimentation électrique et l'air conditionné ;
* les risques de dégât des eaux ;
* la prévention et la protection contre l'incendie ;
* la mémorisation des supports, par exemple, exigeant la mémorisation des supports de mémorisation dans un local séparé qui soit physiquement sûr et protégé des dommages du feu et des eaux ;
* l'évacuation des déchets ;
* une sauvegarde hors site.

4.5.2 Contrôle de la procédure

Dans ce sous composant, on décrit les exigences pour la reconnaissances des rôles de confiance, ainsi que les responsabilités de chaque rôle. Des exemples de rôles de confiance incluent les administrateurs du système, les officiers de sécurité, et les analystes du système.
Pour chaque tâche identifiée, le nombre des individus requis pour effectuer la tâche (règle n parmi m) devrait être déclaré pour chaque rôle. Les exigences d'identification et d'authentification pour chaque rôle peuvent aussi être définies.
Ce composant inclut aussi la séparation des tâches en termes de rôles qui ne peuvent être effectués par les mêmes individus.

4.5.3 Contrôle de sécurité des personnels

Ce sous composant s'adresse à ce qui suit :
* les qualifications, l'expérience, et les habilitations que le personnel doit avoir comme condition pour tenir des rôles de confiance ou d'autres rôles importants. Les exemples incluent les accréditifs, l'expérience de l'emploi, et les habilitations officielles du gouvernement que les candidats à ces positions doivent avoir pour être engagés ;
* les procédures de vérification de fond et des accréditifs qui sont exigées en relation avec l'engagement des personnels tenant les rôles de confiance ou peut-être d'autres rôles importants ; de tels rôles peuvent requérir une vérification de leur casier judiciaire, références, et accréditifs supplémentaires qu'un participant entreprend après qu'à été prise la décision d'engager une certaine personne ;
* les exigences et les procédures de formation pour chaque rôle suivant l'engagement de personnels ;
* la période et les procédures de formation pour chaque rôle après l'achèvement de la formation initiale ;

* la fréquence et la séquence de la rotation des tâches entre les divers rôles ;
* les sanctions contre les personnels pour les actions non autorisées, l'abus d'autorité, et l'utilisation non autorisée des systèmes de l'entité dans le but d'imposer des charges au personnel d'un participant ;
* les contrôles sur le personnel qui sont des contractants indépendants plutôt que des employés de l'entité ; parmi les exemples :
  - les exigences de résidence pour les personnels sous contrat ;
  - les exigences contractuelles incluant l'indemnisation pour dommages dus aux actions du personnel sous contrat ;
  - audit et surveillance du personnel sous contrat ;
  - autres contrôles sur le personnel sous contrat.
* la documentation à fournir au personnel durant la formation initiale, la formation complémentaire, ou autrement.

4.5.4 Procédures d'enregistrement d'audit

Ce sous composant est utilisé pour décrire les systèmes d'enregistrement d'événements et d'audit, mis en œuvre pour maintenir un environnement sûr. Les éléments incluent ce qui suit :

* les types d'événements enregistrés, comme les opérations du cycle de vie des certificats, les tentatives d'accès au système, et les demandes faites au système ;
* la fréquence avec laquelle les enregistrements d'audit sont traités ou archivés, par exemple, toutes les semaines, à la suite d'une alarme ou d'un événement anormal, ou chaque fois que le journal d'audit est rempli à n % ;
* la période pendant laquelle les journaux d'audit sont conservés ;
* la protection des enregistrements d'audit :
  - qui peut voir les enregistrements d'audit, par exemple seulement l'administrateur auditeur ;
  - la protection contre la modification des journaux d'audit, par exemple l'exigence que personne ne puisse modifier ou supprimer les enregistrements d'audit ou que seul un administrateur d'audit puisse supprimer un fichier d'audit au titre de la rotation des fichiers d'audit ;
  - la protection contre la suppression des enregistrements d'audit.
* les procédure de sauvegarde du journal d'audit ;
* si le système d'accumulation des journaux d'audit est interne ou externe à l'entité ;
* si le sujet qui a causé un événement d'audit est notifié de l'action d'audit ;
* l'évaluation des faiblesses, par exemple, lorsque les données d'audit sont traitées dans un outil qui a identifié un potentiel de tentative d'atteinte à la sécurité du système.

v

e4.5.5 Archivage des enregistrements

Ce sous composant est utilisé pour décrire les politiques générales d'archivage des enregistrements (ou rétention d'archives) incluant ce qui suit :

* les types d'enregistrements qui sont archivés par exemple, toutes les données d'audit, les informations de demande de certificat, et la documentation qui prend en charge les demandes de certificat ;
* la période de rétention pour une archive ;
* la protection d'une archive :
  - qui peut voir l'archive, par exemple, l'exigence que seul l'administrateur d'audit puisse la voir ;
  - la protection contre la modification de l'archive, comme une mémorisation sûre des données sur un support en écriture seule ;
  - la protection contre la suppression de l'archive ;
  - la protection contre la détérioration du support de mémorisation de l'archive, comme l'exigence que les données soient déplacées périodiquement sur un support frais ;
  - la protection contre l'obsolescence du matériel, des systèmes d'exploitation, et autres logiciels, en conservant par exemple au titre de l'archive le matériel, les systèmes d'exploitation, et/ou autre logiciel afin de permettre l'accès et l'utilisation des enregistrements archivés à l'avenir.
* les procédures de sauvegarde d'archive ;
* les exigences d'horodatages des enregistrements ;
* si le système de collection d'archive est interne ou externe ;
* les procédures pour obtenir et vérifier les informations d'archive, comme l'exigence que deux copies séparées de l'archive soient conservées sous le contrôle de deux personnes, et que les deux copies soient comparées afin de s'assurer de la précision des informations archivées.

4.5.6 Changement de clés

Ce sous composant décrit les procédures pour fournir une nouvelle clé publique aux utilisateurs d'une CA à la suite d'un changement de clé par la CA. Ces procédures peuvent être les mêmes que celles pour fournir la clé actuelle. Aussi, la nouvelle clé peut être certifiée dans un certificat signé en utilisant la vieille clé.

4.5.7 Récupération sur compromission et désastre

Ce sous composant décrit les exigences relatives à la procédure de notification et de récupération dans l'éventualité d'une compromission ou d'un désastre. Chacun des éléments suivants peut devoir être considéré séparément :

* L'identification ou la liste des incidents applicables et des rapports de compromission et les procédures de traitement.
* Les procédures de récupération utilisées si les ressources informatiques, logiciels, et/ou données sont corrompus ou suspectés d'être corrompus. Ces procédures décrivent comment un environnement sûr est rétabli, quels certificats sont révoqués, si la clé de l'entité est révoquée, comment la nouvelle clé publique de l'entité est fournie aux utilisateurs, et comment les sujets sont re-certifiés.
* Les procédures de récupération utilisées si la clé de l'entité est compromise. Ces procédures décrivent comment un environnement sûr est rétabli, comment la nouvelle clé publique d'entité est fournie aux utilisateurs, et comment les sujets sont re-certifiés.
* Les capacités de l'entité à assurer la continuité des affaires suite à un désastre, naturel ou autre. De telles capacités peuvent inclure la disponibilité d'un site de secours distant sur lequel le fonctionnement peut être restauré. Cela peut aussi inclure des procédures pour sécuriser ses facilités durant la période qui suit un désastre naturel ou autre et avant le rétablissement d'un environnement sûr, soit dans le site d'origine, soit dans un site distant. Par exemple, les procédures pour protéger contre le vol de matériels sensibles sur un site endommagé par un tremblement de terre.

4.5.8 Terminaison de CA ou RA

Ce sous composant décrit les exigences relatives aux procédures de terminaison et de notification de terminaison d'une CA ou RA, incluant l'identité du gardien des enregistrements d'archive de la CA et de la RA.

4.6 Contrôles de la sécurité technique

Ce composant est utilisé pour définir les mesures de sécurité prises par la CA productrice pour protéger ses clés cryptographiques et ses données d'activation (par exemple, les PIN, les mots de passe, ou les clés partagées détenues manuellement). Ce composant peut aussi être utilisé pour imposer des contraintes aux dépôts, aux CA sujettes, aux souscripteurs, et autres participants pour protéger leurs clés privées, les données d'activation pour leurs clés privées, et les paramètres de sécurité critiques. La gestion de clé sécurisée est critique pour assurer que toutes les clés secrètes et privées et les données d'activation sont protégées et ne sont utilisées que par des personnels autorisés.

Ce composant décrit aussi d'autres contrôles techniques de sécurité utilisés par la CA productrice pour effectuer en toute sécurité les fonctions de génération de clé, d'authentification d'utilisateur, d'enregistrement de certificat, de révocation de certificat, d'audit, et d'archivage. Les contrôles techniques incluent les contrôles de sécurité du cycle de vie (incluant la sécurité de l'environnement du développement du logiciel, la méthodologie de développement de logiciel de confiance) et les contrôles de sécurité du fonctionnement.

Ce composant peut aussi être utilisé pour définir d'autres contrôles de sécurité techniques sur les dépôts, les CA sujettes, les RA, les souscripteurs, et autres participants.

4.6.1 Génération et installation de paire de clés

La génération et l'installation des paires de clés doit être considérée pour la CA productrice, les dépôts, les CA sujettes, les RA, et les souscripteurs. Pour chacun de ces types d'entités, les réponses aux questions suivantes peuvent devoir être données :

1. Qui génère la paire de clés d'entité publique, privée ? Les possibilités incluent le souscripteur, la RA, ou la CA. Aussi, comment est effectuée la génération de clé ? La génération de clé est elle effectuée par le matériel ou un logiciel ?
2. Comment la clé privée est elle fournie en toute sécurité à l'entité ? Les possibilités incluent une situation où l'entité l'a générée et donc l'a déjà, la remise physique de la clé privée à l'entité, l'envoi par messagerie d'un jeton contenant la clé privée sécurisée, ou sa livraison dans une session SSL.
3. Comment la clé publique de l'entité est elle fournie en toute sécurité à l'autorité de certification ? Certaines possibilités sont une session SSL en ligne ou un message signé par la RA.
4. Dans le cas de CA productrices, comment la clé publique de la CA est-elle fournie en toute sécurité aux consommateurs d'assertions potentiels ? Les possibilités incluent de passer la clé publique au consommateur d'assertions en personne, d'envoyer physiquement dans un message une copie sécurisée au consommateur d'assertions, ou de la livrer dans une session SSL.
5. Quelles sont les tailles de clés ? Les exemples incluent un module RSA de 1 024 bits et un grand nombre premier DSA de 1 024 bits.
6. Qui génère les paramètres de la clé publique, et la qualité des paramètres est-elle vérifiée durant la génération de la clé ?
7. À quelles fins la clé peut elle être utilisée, ou pour quel objet l'usage de la clé doit il être interdit ? Pour les certificats X.509, leur objet devrait correspondre aux fanions d'usage de clé des certificats de X.509 version 3.

4.6.2 Protection de clé privée et contrôle de l'ingénierie de module cryptographique

Les exigences sur la protection des clés privées et des modules cryptographiques doivent être prises en considération par la CA productrice, les dépôts, les CA sujettes, les RA, et les souscripteurs. Pour chacun de ces types d'entités, il peut être nécessaire de donner des réponses aux questions suivantes :

1. Quelles normes, si il en est, sont exigées pour le module cryptographique utilisé pour générer les clés ? Un module cryptographique peut être composé de matériel, de logiciel, de progiciels, ou de toutes leurs combinaisons. Par exemple, est-il exigé que les clés certifiées par l'infrastructure soient générées en utilisant des modules conformes à la norme US FIPS 140-1 ? Si oui, quel est le niveau de FIPS 140-1 exigé du module ? Y a-t-il d'autres contrôles d'ingénierie ou autres relatifs à un module cryptographique, comme l'identification de la frontière du module cryptographique, l'entrée/sortie, les rôles et services, l'automate à états finis, la sécurité physique, la sécurité logicielle, la sécurité du système d'exploitation, la conformité des algorithmes, la compatibilité électromagnétique, et l'auto vérification ?
2. La clé privée est –elle sous le contrôle de n parmi m personnes ? (7) Si oui, donner n et m (le contrôle par deux personnes est un cas particulier de n parmi m, où n = m = 2) ?
3. La clé privée est elle sous la garde d'un tiers de confiance ? (8) Si oui, qui est le tiers de confiance, sous quelle forme la clé est elle gardée (les exemples incluent le texte en clair, chiffré, clé partagée) et quels sont les contrôles de sécurité sur le système de tiers de confiance ?
4. La clé privée est elle sauvegardée ? Si elle l'est, qui est l'agent de sauvegarde, sous quelle forme la clé est-elle sauvegardée (les exemples incluent le texte en clair, le chiffrage, la clé partagée) et quels sont les contrôles de sécurité sur le système de sauvegarde ?
5. La clé privée est-elle archivée ? Si oui, qui est l'agent d'archivage, sous quelle forme la clé est-elle archivée (les exemples incluent le texte en clair, chiffré, clé partagée) et quels sont les contrôles de sécurité sur le système d'archivage ?
6. Dans quelles circonstances, si il en est, une clé privée peut elle être transférée dans ou d'un module cryptographique ? À qui est-il permis d'effectuer une telle opération de transfert ? Sous quelle forme est la clé privée durant le transfert (c'est-à-dire, texte en clair, chiffré, ou clé partagée) ?
7. Comment la clé privée est elle mémorisée dans le module (c'est-à-dire, texte en clair, chiffré, ou clé partagée) ?
8. Qui peut activer (utiliser) la clé privée ? Quelles actions doivent être effectuées pour activer la clé privée (par exemple, connexion, mise sous tension, fournir un PIN, insérer un jeton/clé, automatique, etc.) ? Une fois la clé activée, est elle active pour un délai indéfini, pour une seule fois, ou pour un délai défini ?
9. Qui peut désactiver la clé privée et comment ? Des exemples de méthodes de désactivation de clés privées incluent la déconnexion, la mise hors tension, le retrait du jeton/clé, la désactivation automatique, et l'expiration du délai.
10. Qui peut détruire la clé privée et comment ? Des exemples de méthodes de destruction de clés privées incluent la restitution du jeton, la destruction du jeton, et l'écrasement de la clé.
11. Fournir les capacités du module cryptographique dans les zones suivantes : identification de la limite du module cryptographique, entrée/sortie, rôles et services, automate à états finis, sécurité physique, sécurité logicielle, sécurité du système d'exploitation, conformité des algorithmes, compatibilité électromagnétique, et auto vérification. La capacité peut être exprimée par référence à la conformité avec une norme comme U.S. FIPS 140-1, le niveau associé, et le grade.

4.6.3 Autres aspects de la gestion de paire de clés

D'autres aspects de la gestion de clé doivent être considérés pour la CA productrice, les dépôts, les CA sujettes, les RA, les souscripteurs, et autres participants. Pour chaque type d'entité, on peut devoir fournir les réponses aux questions suivantes :

1. La clé publique est-elle archivée ? Si oui, qui est l'agent d'archivage et quels sont les contrôles de sécurité sur le système d'archivage ? Aussi, quels logiciels et matériels doivent être préservés au titre de l'archivage pour permettre l'utilisation de la clé publique à l'avenir ? Note : ce sous composant ne se limite pas à exiger de décrire l'utilisation de signatures numériques sur des données d'archives, mais s'adresse plutôt aux contrôles d'intégrité autres que les signatures numériques lorsque une archive exige une protection contre l'altération. Les signatures numériques ne fournissent pas de protection contre l'altération ni ne protègent l'intégrité des données ; elles vérifient simplement l'intégrité des données. De plus, la période d'archivage peut être supérieure à la période de cryptanalyse de la clé publique nécessaire pour vérifier une signature numérique appliquée aux données d'archive.
2. Quelle est la durée opérationnelle du certificats produit au souscripteur. Quelle est la période d'usage, ou la durée de vie active, de la paire de clés du souscripteur ?

4.6.4 Données d'activation

Les données d'activation se réfèrent aux valeurs de données autres que de clés privées exigées pour opérer sur des clés privées ou des modules cryptographiques contenant des clés privées, comme un PIN, une phrase de passe, ou des portions d'une clé privée utilisée dans un schéma de partage de clé. La protection des données d'activation empêche l'utilisation non autorisée de la clé privée, et a potentiellement besoin d'être considérée pour la CA productrice, les CA sujettes, les RA, et les souscripteurs. Une telle considération peut devoir s'adresser à la totalité du cycle de vie des données d'activation, de leur génération à l'archivage et la destruction. Pour chacun des types d'entité (CA productrice, dépôt, CA sujette, RA, souscripteur, et autres

participants) toutes les questions énumérées aux paragraphes 4.6.1 à 4.6.3 peuvent devoir nécessiter des réponses à l'égard des données d'activation plutôt qu'à l'égard des clés.

4.6.5 Contrôle de la sécurité informatique

Ce sous composant est utilisé pour décrire des contrôles de sécurité informatique tels que : l'utilisation du concept de base informatique de confiance, de contrôle d'accès discrétionnaire, d'étiquettes, de contrôles d'accès obligatoires, de réutilisation d'objet, d'audit, d'identification et authentification, de chemin de confiance, de vérification de la sécurité, et de vérification de pénétration. L'assurance du produit peut aussi être traitée.

Un classement de la sécurité informatique pour les systèmes d'ordinateurs peut être exigé. Le classement pourrait se fonder, par exemple, sur les critères d'évaluation de systèmes de confiance (TCSEC, *Trusted System Evaluation Criteria*), les critères canadiens d'évaluation des produits de confiance, sur les critères européens d'évaluation de la sécurité des technologies de l'information (ITSEC, *Information Technology Security Evaluation Criteria*), ou sur les critères communs pour l'évaluation de la sécurité des technologies de l'information de la norme ISO/CEI 15408:1999. Ce sous composant peut aussi établir des exigences pour l'analyse de l'évaluation de produits, les essais, les profils, la certification de produit, et/ou l'accréditation de produit entreprise sur les activités en rapport.

4.6.6 Contrôle de la sécurité du cycle de vie

Ce sous composant s'adresse au contrôle du développement du système et aux contrôles de la gestion de la sécurité.

Les contrôles du développement de système incluent la sécurité de l'environnement de développement, la sécurité du personnel de développement, la sécurité de la gestion de la configuration durant la maintenance du produit, les pratiques d'ingénierie du logiciel, la méthodologie de développement du logiciel, la modularité, la mise en couches, l'utilisation de techniques de conception et de mise en œuvre sans défaillance (par exemple, programmation défensive) et sécurité des locaux de développement.

Les contrôles de la gestion de la sécurité incluent l'exécution d'outils et procédures pour assurer que les systèmes et réseaux opérationnels adhèrent à la sécurité configurée. Ces outils et procédures incluent de vérifier l'intégrité du logiciel, progiciel et matériel de sécurité pour s'assurer de leur fonctionnement correct.

Ce sous composant peut aussi s'adresser aux classements de la sécurité du cycle de vie sur la base, par exemple, de la méthodologie de développement de logiciel de confiance (TSDM, *Trusted Software Development Methodology*) niveaux IV et V, de l'audit indépendant de contrôles de sécurité du cycle de vie, et le modèle de maturité de capacité de l'institut d'ingénierie du logiciel (SEI-CMM, *Software Engineering Institute's Capability Maturity Model*).

4.6.7 Contrôle de la sécurité du réseau

Ce sous composant s'adresse aux contrôles relatifs à la sécurité du réseau, incluant les pare-feu.

4.6.8 Horodatage

Ce sous composant s'adresse aux exigences ou pratiques relatives à l'utilisation d'horodatages sur diverses données. Il peut aussi discuter si l'application d'horodatage doit utiliser une source horaire de confiance.

4.7 Profils de certificat et de CRL

Ce composant est utilisé pour spécifier le format de certificat et, si des CRL et/ou OCSP sont utilisées, le format de CRL et/ou d'OCSP. Cela inclut les informations sur les profils, versions, et extensions utilisés.

4.7.1 Profils de certificat

Ce sous composant s'adresse aux sujets suivants (éventuellement par référence à une définition de profil séparée, comme celle définie dans la RFC3280) :

* Numéros de version supportés ;
* Extensions de certificat remplies et leur criticité ;
* Identifiants d'objet d'algorithme cryptographique ;
* Formes de noms utilisées pour les noms de CA, RA, et souscripteur ;
* Contraintes de nom utilisées et formes de noms utilisées dans les contraintes de noms ;

* OID de CP applicables ;
* Usage d'extension de contraintes de politique ;
* Syntaxe et sémantique des qualificatifs de politique ;
* Sémantique du traitement de l'extension de CP critique.

4.7.2 Profils de CRL

Ce sous composant s'adresse à des sujets comme ceux qui suivent (éventuellement par référence à une définition de profil séparée, comme celle définie dans la RFC3280) :

* Numéros de version supportés pour les CRL ;
* CRL et extensions d'entrées de CRL remplies et leur criticité.

4.7.3. Profil OCSP

Ce sous composant s'adresse à des sujets comme ceux qui suivent (éventuellement par référence à une définition de profil séparée, comme celle définie dans le profil de la RFC2560) :

* Version d'OCSP utilisée comme base d'établissement d'un système OCSP ;
* Extensions OCSP remplies et leur criticité.

4.8 Audit de conformité et autres vérifications

Ce composant s'adresse à ce qui suit :

* Liste des sujets couverts par l'attestation et/ou méthodologie d'attestation utilisée pour effectuer l'attestation ; les exemples incluent WebTrust pour les CA (9) et SAS 70 (10).
* Fréquence des audits de conformité ou autre attestation pour chaque entité qui doit être évaluée selon une CP ou CPS, ou circonstances qui déclenchent une évaluation ; les possibilités incluent un audit annuel, une évaluation avant la mise en fonctionnement comme condition d'autoriser le fonctionnement de l'entité, ou investigation suivant une éventuelle ou réelle compromission de la sécurité.
* Identité et/ou qualifications du personnel effectuant l'audit ou autre évaluation.
* Relations entre l'évaluateur et l'entité évaluée, incluant le degré d'indépendance de l'évaluateur.
* Actions entreprises par suite des déficiences trouvées durant l'évaluation ; par exemple une suspension temporaire de fonctionnement jusqu'à la correction des déficiences, révocation des certificats produits par l'entité évaluée, changements du personnel, déclenchement d'investigations spéciales ou évaluations de conformité plus fréquentes à l'avenir, et demandes de réparations à l'entité évaluée.
* Qui est habilité à voir les résultats d'une évaluation (par exemple, l'entité évaluée, les autres participants, le public) qui les leur fournit (par exemple, l'évaluateur ou l'entité évaluée) et comment ils sont communiqués.

4.9 Autres problèmes d'affaires et juridiques

Ce composant couvre les affaires générales et juridiques. Les paragraphes 9.1 et 9.2 du cadre discutent les questions de frais à facturer pour les divers services et la responsabilité financière des participants pour maintenir les ressources des opérations courantes et pour payer les jugements ou accords en réponse aux plaintes formulées contre eux. Les paragraphes restants sont en relations avec les questions juridiques.

En commençant au paragraphe 9.3 du cadre, l'ordre des sujets est le même que, ou est similaire à, l'ordre des sujets d'un accord normal de licence de logiciel ou autre accord technologique. Par conséquent, ce cadre peut non seulement être utilisé pour les CP et CPS, mais aussi pour les accords associés en relation avec la PKI, en particulier les accords de souscripteurs, et les accords de consommateur d'assertions. Cet ordre est destiné à aider la relecture par des juristes des CP, CPS, et autres documents qui adhèrent à ce cadre.

Par rapport à beaucoup des sous composants juridiques au sein de ce composant, un rédacteur de CP ou CPS peut choisir d'inclure dans le document des termes et conditions qui s'appliquent directement aux souscripteurs ou consommateurs d'assertions. Par exemple, une CP ou CPS peut déclarer des limitations de responsabilité qui s'appliquent aux souscripteurs et consommateurs d'assertions. L'inclusion de termes et conditions sera vraisemblablement appropriée lorsque la CP ou CPS est elle-même un contrat ou une partie d'un contrat.

Dans d'autres cas, cependant, la CP ou CPS n'est pas un contrat ni une partie d'un contrat ; elle est plutôt configurée de telle sorte que ses termes et conditions sont appliqués aux parties par des documents séparés, qui peuvent inclure des accords associés, comme un accord de souscripteur ou consommateur d'assertions. Dans ce cas, un rédacteur de CP peut souhaiter

écrire une CP de façon que certains termes et conditions juridiques apparaissent (ou non) dans de tels accords associés. Par exemple, une CP pourrait inclure un sous composant déclarant qu'un certain terme de limitation de responsabilité doit apparaître dans un accord de souscripteur et consommateur d'assertions de CA. Un autre exemple est celui d'une CP qui contient un sous composant qui interdit l'utilisation d'un accord de souscripteur ou consommateur d'assertions contenant une limitation de la responsabilité de la CA incompatible avec les dispositions de la CP. Un rédacteur de CPS peut utiliser des sous composants juridiques pour révéler que certains termes et conditions apparaissent dans les accords associés de souscripteur, consommateur d'assertions, ou autres utilisés par la CA. Une CPS peut expliquer, par exemple, que la rédaction de la CA utilise un accord de souscripteur ou consommateur d'assertions associé qui applique une disposition particulière pour limiter la responsabilité.

4.9.1 Redevances

Ce sous composant contient toutes les dispositions applicables concernant les redevances appliquées par les CA, dépôts, ou RA, comme :

* les frais de production ou renouvellement de certificat ;
* les redevances d'accès au certificat ;
* les redevances de révocation ou d'accès aux informations d'état ;
* les redevances pour les autres services comme la fourniture de l'accès à la CP ou CPS pertinente ;
* la politique de refinancement.

4.9.2 Responsabilité financière

Ce sous composant contient les exigences ou dispositions relatives aux ressources disponibles pour les CA, RA, et autres participants qui fournissent des services de certification à l'appui de leurs responsabilités dans le fonctionnement de la PKI, et pour rester solvables et payer des dommages en cas de reconnaissance de leur responsabilité par un jugement ou un accord en rapport avec une plainte résultant de ces opérations. Ces dispositions incluent :

* une déclaration que le participant conserve une certaine couverture d'assurance pour sa responsabilité à l'égard des autres participants ;
* une déclaration qu'un participant a accès à d'autres ressources pour prendre en charge les opérations et payer les dommages qui pourraient lui être imputés, qui peuvent être rédigées en termes d'un niveau minimum de ressources nécessaires pour fonctionner et couvrir les dépenses contingentes qui pourraient survenir dans une PKI, où les exemples incluent des biens dans la comptabilité d'une organisation, des obligations, une lettre de crédit, et un droit, dans un accord, à une indemnité dans certaines circonstances ;
* une déclaration qu'un participant a un programme qui offre une assurance pour les tiers ou une garantie de protection aux autres participants en connexion avec leur utilisation de la PKI.

4.9.3 Confidentialité des informations d'affaires

Ce sous composant contient des dispositions relatives au traitement des informations d'affaires confidentielles que les participants peuvent se communiquer les uns aux autres, comme un programme d'actions, des informations sur les ventes, des secrets commerciaux, et des information reçues de tiers sous un accord de non divulgation. Précisément, ce sous composant s'adresse à :

* la portée de ce qui est considéré comme des informations confidentielles,
* les types d'informations qui sont considérées comme sortant du cadre des informations confidentielles,
* les responsabilités des participants qui reçoivent des informations confidentielles pour empêcher leur compromission, et s'abstenir de les utiliser avec des tiers ou de les leur divulguer.

4.9.4 Confidentialité des informations personnelles

Ce sous composant se rapporte à la protection que les participants, en particulier les CA, RA, et dépôts, peuvent être obligés d'assurer sur les informations privées sur des personnes identifiables des demandeurs de certificats, souscripteurs, et autres participants. Précisément, ce sous composant s'adresse à ce qui suit, dans la mesure pertinente des lois applicables :

* la désignation et divulgation du plan de confidentialité applicable qui s'applique aux activités du participant, si c'est exigé par la loi ou politique applicable ;
* les informations qui sont considérées comme privées ou non au sein de la PKI ;
* toute responsabilité des participants qui reçoivent des informations privées de les sécuriser, et de s'abstenir de les utiliser et de les divulguer à des tiers ;
* toutes les exigences de remarques ou consentement des individus concernant l'utilisation des informations privées ;
* toutes les circonstances dans lesquelles un participant est habilité à, ou requis de, divulguer des informations privées suite à un processus judiciaire, ou administratif ou gouvernemental, ou dans toutes procédures légales.

4.9.5 Droits de propriété intellectuelle

Ce sous composant s'adresse aux droits de propriété intellectuelle, tels que les droits de reproduction, brevets, marques commerciales, ou secrets commerciaux, que certains participants peuvent avoir ou revendiquent dans une CP, CPS, certificats, noms, et clés, ou sont l'objet d'une licence des ou aux participants.

4.9.6 Représentations et garanties

Ce sous composant peut inclure les représentations et garanties de diverses entités faites conformément à la CP ou CPS. Par exemple, une CPS qui sert de contrat peut contenir une garantie de la CA que les informations contenues dans le certificat sont exactes. Autrement, une CPS peut contenir une garantie moins étendue disant que les informations contenues dans le certificat sont véridiques pour autant que le sache la CA après avoir effectué certaines procédures d'authentification d'identité avec la diligence convenable. Ce sous composant peut aussi inclure des exigences que les représentations et garanties apparaissent dans certains accords, comme les accords de souscripteur ou de consommateur d'assertions. Par exemple, une CP peut contenir l'exigence que toutes les CA utilisent un accord de souscripteur, et qu'un accord de souscripteur doit contenir une garantie de la CA que les informations du certificat sont exactes. Les participants qui font des représentations et garanties incluent les CA, RA, souscripteurs, consommateurs d'assertions, et autres participants.

4.9.7 Déclinatoires de garanties

Ce sous composant peut inclure des déclinatoires exprès de garantie qui peuvent autrement être réputés exister dans un accord, et des déclinatoires de garanties implicites qui peuvent autrement être imposées par la législation applicable, comme des garanties de commercialisation ou d'adéquation à un objet particulier. La CP ou CPS peut imposer directement de tels déclinatoires, ou la CP ou CPS peut contenir l'exigence que les déclinatoires apparaissent dans des accords associés, comme des accords de souscripteur ou de consommateur d'assertions.

4.9.8 Limitations de responsabilité

Ce sous composant peut inclure des limitations de responsabilité dans une CP ou CPS ou des limitations qui apparaissent ou doivent apparaître dans un accord associé à la CP ou CPS, comme un accord de souscripteur ou de consommateur d'assertions. Ces limitations peuvent entrer dans une des deux catégories suivantes : limitations sur les éléments de dommages récupérables et limitations sur la quantité de dommages récupérables, aussi appelées limitations de responsabilité. Souvent, les contrats contiennent des clauses empêchant le recouvrement des éléments de dommages tels que des dommages incidents et conséquents, et parfois des dommages punitifs. Fréquemment, les contrats contiennent des clauses qui limitent le possible recouvrement d'une partie ou de l'autre à une certaine quantité ou à une quantité correspondant à un repère, comme la somme payée au vendeur à la signature du contrat.

4.9.9 Indemnités

Ce sous composant inclut des dispositions par lesquelles une des parties accorde à une seconde des indemnités pour pertes ou dommages subis par cette seconde partie, résultant normalement de la conduite de la première partie. Elles peuvent apparaître dans une CP, CPS, ou un accord. Par exemple, une CP peut exiger qu'un accord de souscripteurs contienne une clause par laquelle un souscripteur est responsable de l'indemnisation d'une CA pour les pertes subies par la CA suite des renseignements frauduleux d'un souscripteur sur la demande de certificat sous laquelle la CA a produit au souscripteur un certificat inapproprié. De même, une CPS peut dire qu'une CA utilise un accord de consommateur d'assertions, dans lequel le consommateurs d'assertions est responsable de l'indemnisation d'une CA pour les pertes subies par la CA suite à l'utilisation d'un certificat sans une vérification appropriée des informations de révocation ou l'utilisation d'un certificat pour des objets non permis par la CA.

4.9.10 Terme et terminaison

Ce sous composant peut inclure la période pendant laquelle la CP ou CPS reste en vigueur et les circonstances dans lesquelles le document, des portions du document, ou son applicabilité à un participant particulier peuvent se terminer. En plus, ou autrement, la CP ou CPS peut inclure l'exigence que certain terme et clause de terminaison apparaissent dans les accords, comme des accord de souscripteur ou consommateur d'assertions. En particulier, ces clauses peuvent inclure :

* le terme d'un document ou d'un accordent, c'est-à-dire quand le document devient effectif et quand il arrive à expiration si il ne s'est pas terminé antérieurement ;
* les dispositions de terminaison qui déclarent les circonstances dans lesquelles le document, certaines de ses portions, ou son application à un participant particulier cessent de rester en vigueur ;
* toutes les conséquences de la terminaison du document. Par exemple, certaines dispositions d'un accord peuvent survivre à sa terminaison et rester en vigueur. Des exemples incluent des reconnaissances de droits de propriété intellectuelle et des dispositions de confidentialité. Aussi, la terminaison peut déclencher une responsabilité des parties pour retourner des

informations confidentielles à la partie qui les a divulguées.

4.9.11 Notices individuelles et communications avec les participants

Ce sous composant discute la façon dont un participant peut ou doit communiquer de façon bilatérale avec un autre participant afin que ces communications aient une valeur juridique. Par exemple, une RA peut souhaiter informer la CA qu'elle désire mettre fin à son accord avec cette CA. Ce sous composant est différent des fonctions de publication et de dépôt, parce que, à la différence des communications individuelles décrites dans ce sous composant, la publication et l'envoi à un dépôt sont pour les besoins des communications à large audience de récepteurs, comme le sont tous les consommateurs d'assertions. Ce sous composant peut établir des mécanismes pour communiquer et indiquer les informations de contact à utiliser pour de telles communications, comme des notices de messages électroniques signées numériquement à une adresse spécifiée, suivie par un accusé de réception par message électronique signé numériquement.

4.9.12 Amendements

Il sera à l'occasion nécessaire d'amender une CP ou CPS. Certains de ces changements ne vont pas réduire matériellement l'assurance qu'une CP ou sa mise en œuvre fournit, et sera jugée par l'administrateur de la politique comme ayant un effet insignifiant sur l'acceptabilité des certificats. De tels changements à une CP ou CPS n'ont pas besoin d'exiger un changement de l'OID de la CP ou du pointeur de la CPS (URL). D'un autre côté, certains changements d'une spécification vont changer matériellement l'acceptabilité des certificats pour des besoins spécifiques, et ces changements peuvent exiger des changements correspondants de l'OID de la CP ou du qualificatif du pointeur de la CPS (URL).

Ce sous composant peut aussi contenir les informations suivantes :

* Les procédures par lesquelles la CP ou CPS et/ou autres documents doivent être, peuvent être, ou sont amendés. Dans le cas d'amendements de CP ou CPS, les procédures de changement peuvent inclure un mécanisme de notification pour notifier les amendements proposés aux parties affectées, comme les souscripteurs et consommateurs d'assertions, une période de commentaires, un mécanisme par lequel les commentaires sont reçus, révisés et incorporés dans le document, et un mécanisme par lequel les amendements sont finalisés et entrent en vigueur.
* Les circonstances dans lesquelles les amendements à la CP ou CPS vont exiger un changement de l'OID de la CP ou du pointeur de CPS (URL).

4.9.13 Procédures de résolution de conflit

Ce sous composant discute les procédures utilisées pour résoudre les conflits survenant sur la CP, CPS, et/ou accords. Des exemples de ces procédures incluent l'exigence que les conflits soient résolus dans un certain forum ou par d'autres mécanismes de résolution de conflit.

4.9.14 Juridiction compétente

Ce sous composant prévoit une déclaration que une certaine juridiction gouverne l'interprétation et la mise en application de la CP ou CPS sujette ou des accords.

4.9.15 Conformité à la loi applicable

Ce sous composant est relatif aux exigences déclarées que les participants se conforment aux lois applicables, par exemple, les lois relatives au matériel et logiciel cryptographique qui peuvent être soumis aux lois sur le contrôle des exportations d'une certaine juridiction. La CP ou CPS pourrait prétendre imposer de telles exigences ou peut exiger que de telles dispositions apparaissent dans d'autres accords.

4.9.16 Dispositions diverses

Ce sous composant contient des dispositions diverses, parfois appelées "dispositions fourre-tout" dans les contrats. Les clauses couvertes par ce sous composant peuvent apparaître dans une CP, CPS, ou accord et incluent :

* une clause d'accord entier, qui identifie normalement le ou les documents composant l'accord entier entre les parties et déclare que de tels accords se substituent à tout arrangement antérieur et contemporain écrit ou oral en rapport avec le même sujet ;
* une clause d'affectation, qui peut agir pour limiter la capacité d'une partie à un accord, affectant ses droits dans l'accord à une autre partie (comme le droit de recevoir des payements à l'avenir) ou limitant la capacité d'une partie à déléguer ses obligations relatives à l'accord ;
* une clause de réduction, qui précise les intentions des parties au cas où une juridiction ou autre tribunal déterminerait qu'une clause d'un accord serait, pour une raison quelconque, invalide ou inapplicable, et dont l'objet est fréquemment

d'empêcher l'inapplicabilité d'une clause de causer l'inapplicabilité de tout l'accord ;

* une clause de mise en application qui peut déclarer qu'une partie qui l'emporte dans tout conflit au sujet d'un accord est en droit de recevoir des indemnités au titre de ses dommages, ou peut déclarer que le renoncement d'une partie à une rupture du contrat ne constitue pas une renonciation continue ou future à d'autres infractions au contrat.
* une clause de force majeure, couramment utilisée pour excuser les performances d'une ou plusieurs parties à un accord dues à un événement sortant du contrôle raisonnable de la ou des parties affectées. Normalement, la durée de l'excuse est en rapport avec la durée du retard causé par l'événement. La clause peut aussi prévoir la terminaison de l'accord dans des circonstances et conditions spécifiées. Les événements considérés comme constituant un cas de "force majeure" peuvent inclure ce qu'on appelle des "actes de Dieu", des guerres, des actes de terrorisme, des grèves, des désastres naturels, des ruptures d'approvisionnement et la défaillance d'un fabricant, ou des défaillances de l'Internet ou autres infrastructure. Les clauses de force majeure devraient être rédigées de façon à être en cohérence avec les autres portions du cadre et accords de niveau de service applicables. Par exemple, les responsabilités et capacités pour la continuité de affaires et la récupération après un désastre peuvent placer certains événements sous le contrôle raisonnable des parties, comme l'obligation d'avoir des sauvegardes d'alimentation électrique en présence de pannes de courant.

4.9.17. Autres dispositions

Ce sous composant est une clause "fourre-tout" où des responsabilités supplémentaires peuvent être imposées aux participants à la PKI qui ne rentrent pas dans un des autres composants ou sous composants du cadre. Les rédacteurs de CP et CPS peuvent placer dans ce sous composant toute disposition qui n'est pas couverte par un autre sous composant.

5. Considérations sur la sécurité

Selon X.509, une politique de certificat (CP, *certificate policy*) est "un ensemble désigné de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou classe d'applications avec des exigences communes de sécurité". Une CP peut être utilisée par un consommateur d'assertions pour l'aider à décider si un certificat, et le lien qu'il contient, sont suffisamment de confiance et par ailleurs appropriés pour une application particulière.

Le degré de confiance que peut accorder le consommateur d'assertions au lien incorporé dans un certificat dépend de plusieurs facteurs. Ces facteurs peuvent inclure les pratiques suivies par l'autorité de certification (CA) pour l'authentification du sujet, de la politique de fonctionnement de la CA, de ses procédures, et des contrôles de sécurité techniques, incluant la portée des responsabilités du souscripteur (par exemple, pour protéger la clé privée) et les responsabilités déclarées et les termes et conditions de responsabilité de la CA (par exemple, garanties, déclinatoires de garanties, et limitations de responsabilité).

Le présent document donne un cadre pour traiter les aspects techniques, procéduraux, personnels, et physiques de la sécurité des modules cryptographiques des autorités de certification, des autorités d'enregistrement, des répertoires, des souscripteurs, et des consommateurs d'assertions, afin d'assurer que la génération, publication, renouvellement, changement de clés, usage, et révocation des certificats sont faits de manière sûre. Précisément, le paragraphe 4.3 Identification et authentification, le paragraphe 4.4 Exigences de fonctionnement du cycle de vie d'un certificat, le paragraphe 4.5 Gestion des facilités et contrôles du fonctionnement, le paragraphe 4.6 Contrôle de la sécurité technique, le paragraphe 4.7 CRL de certificat et profils d'OCSP, et le paragraphe 4.8 Audit de conformité et autres vérifications, sont orientés vers l'assurance d'un fonctionnement sûr des entités de PKI telles que la CA, la RA, les systèmes de répertoire, de souscripteur, et les systèmes de consommateur d'assertions.

6. Esquisse d'un ensemble de dispositions

La présente Section contient une esquisse recommandée pour un ensemble de dispositions, destinée à servir de liste de contrôle ou (avec quelques autres développements) de gabarit standard à utiliser par les auteurs de CP ou de CPS. Une telle esquisse commune facilitera :

(a) La comparaison de deux politiques de certificat durant une certification croisée ou d'autres formes d'interopération (pour les besoins d'une transposition équivalente).
(b) La comparaison d'une CPS avec une CP pour s'assurer que la CPS met loyalement en œuvre la politique.
(c) La comparaison de deux CPS.

Pour se conformer à la RFC, les auteurs d'une CP ou CPS conforme sont invités à suivre cette esquisse. Bien que l'utilisation d'une autre esquisse soit déconseillée, elle peut être acceptée si une justification appropriée est fournie pour s'en écarter et un tableau de transposition est présenté pour discerner directement où chaque élément décrit dans cette esquisse est fourni.

1. Introduction

7. Comparaison avec la RFC 2527

Le présent cadre représente une amélioration par ajouts à la RFC 2527. Le nouveau cadre bénéficie de l'expérience accumulée au cours du déploiement des documents de CP et CPS dans la RFC 2527. De plus, ce nouveau cadre se fonde sur la coordination avec le comité de sécurité de l'information *(ISC)* de l'American Bar Association au sein de la Loi sur la section des Sciences et de la Technologie *(des USA)*. L'ISC a écrit les lignes directrices sur l'évaluation de PKI [ABA2], qui incorpore une grande expérience technique, commerciale, et juridique dans le fonctionnement de la PKI. En particulier, des représentants de l'ISC ont fait des changements au cadre pour qu'il s'inscrive mieux dans l'environnement juridique et le rendre plus accessible aux juristes.

D'un point de vue technique, les changements au cadre de la RFC 2527 sont minimes et s'y ajoutent, plutôt qu'ils ne la révolutionnent. Les Sections 3 à 7 ont largement été préservées, avec une modeste réorganisation et de nouveaux sujets. Par exemple, le nouveau cadre inclut une révision de la Section 4 du cadre pour inclure un traitement complet du cycle de vie du certificat, l'ajout du tiers de confiance, de l'encapsulation de clé, et des politiques et pratiques de récupération de clé, et OCSP. Les fonctions d'audit de la Section 2 apparaissent maintenant seules à la Section 8, et la Section 2 se concentre exclusivement sur les fonctions de dépôt. Les questions d'affaires et juridiques de la Section 2 de la RFC 2527 apparaissent maintenant dans une nouvelle Section 9.

D'un point de vue juridique, la nouvelle Section 9 est utile parce qu'elle place les sujets du cadre dans un ordre qui est similaire à celui des licences de logiciels et autres accords de technologie et est donc familier aux juristes technologiques. De plus, le cadre dans son ensemble peut servir à un accord de souscripteur, consommateur d'assertions, ou autre en rapport avec la PKI. Les changements sont destinés à faire une revue juridique plus efficace, et des apports, aux documents de CP et CPS. La Section 9 ajoute aussi de nouveaux sujets juridiques, comme la confidentialité des informations personnelles, les clauses de responsabilité, et l'efficacité du document.

La Section 1 du nouveau cadre est largement la même que celle de la RFC 2527, bien qu'elle accroisse la couverture des participants à la PKI en séparant les souscripteurs des consommateurs d'assertions et en ajoutant un paragraphe sur les autres participants. Elle change le paragraphe "applicabilité" en un paragraphe qui couvre les utilisations appropriées et interdites des certificats. Elle déplace aussi les procédures d'approbation de CPS du paragraphe 8.3 de la RFC 2527 en un paragraphe sur l'administration de la politique. Finalement, le paragraphe 1.6 ajoute une liste des définitions et acronymes.

La Section 2 du nouveau cadre est une réorganisation du paragraphe 2.6 de l'ancien cadre. La Section 3 du nouveau cadre se fonde sur une division de l'ancien paragraphe 3.1 en deux parties pour les questions de désignation et d'identification et authentification. Elle ajoute de nouvelles questions, comme celle de permettre les pseudonymes et l'anonymat. Les sujets de l'ancienne Section 4 sur les enregistrements d'audit, les archives d'enregistrements, changements de clé, récupération sur compromission et désastre, et la terminaison de CA ont été déplacés à la Section 5. Le reste des sujets de la Section 4 a été développé et réorganisé pour couvrir un cycle de vie complet de certificat. Les nouveaux sujets incluent les éléments implicites dans la Section 4 de la RFC 2527, mais maintenant explicites, tels que le traitement d'une demande de certificat, la modification de certificat, et la fin d'abonnement.

Les nouveaux paragraphes 5.1 à 5.3 sont presque identiques à leur contrepartie de la RFC 2527. Les restes de la nouvelle Section 5 sont les sujets déplacés de la Section 4 de la RFC 2527, dans l'ordre dans lequel ils apparaissaient dans la Section 4. La Section 6 du nouveau cadre est presque la même que l'ancienne Section 6, avec quelques exceptions, comme la

consolidation de l'ancien paragraphe 6.8 (contrôles de l'ingénierie du module cryptographique) dans le paragraphe 6.2.1 (maintenant appelé "Normes et contrôles du module cryptographique") et l'ajout de l'horodatage dans un nouveau paragraphe 6.8. La Section 7 est presque identique à l'ancienne, le changement majeur étant l'ajout d'un paragraphe sur le profil OCSP. La Section 8 est presque identique au paragraphe 2.7 de la RFC 2527.

La nouvelle Section 9 contient les sujets d'affaires et juridiques qui étaient couverts par la Section 2 de la RFC 2527, incluant les redevances, la responsabilité financière, la confidentialité, et la propriété intellectuelle. Elle ajoute un paragraphe sur la confidentialité des informations personnelles, qui est devenue une question significative de politique. Le paragraphe 2.2 "Responsabilité" de la RFC 2527 apparaît maintenant dans les paragraphes 9.6 à 9.9, couvrant les représentations et garanties, les déclinatoires, limitations de responsabilité, et les indemnités. Le paragraphe 9.10 ajouté concerne la durée de l'efficacité de la documentation. Le paragraphe 9.12 collecte les termes concernant la façon dont un document (CP, CPS, accord, ou autre document) peut être amendé, qui apparaissaient anciennement au paragraphe 8.1. La Section 9 inclut les sujets "juridiques passe-partout", dont certains figuraient dans l'ancienne Section 2. Finalement, le paragraphe 9.17 est un fourre-tout "autres dispositions" où les rédacteurs peuvent placer des informations qui ne rentrent pas dans les autres sections du cadre.

La matrice ci-dessous montre les paragraphes du vieux cadre de la RFC 2527 et les paragraphes qui leur succèdent dans le nouveau cadre.

Paragraphe original de la RFC 2527	**Nouveau paragraphe**
1. Introduction	1.
1.1 Généralités	1.1
1.2 Identification	1.2
1.3 Communauté et applicabilité	1.3
1.3.1 Autorités de certification	1.3.1
1.3.2 Autorités d'enregistrement	1.3.2
1.3.3 Entités d'extrémité	1.3.3, 1.3.4
1.3.4 Applicabilité	1.4, 4.5
1.4 Contacts	1.5
1.4.1 Organisation de l'administration de la spécification	1.5.1
1.4.2 Personne à contacter	1.5.2
1.4.3 Personne déterminant la CPS pour la politique	1.5.3
2. Dispositions générales	2, 8, 9
2.1 Obligations	2.6.4
2.1.1 Obligations de la CA	Intégré dans les portions du cadre qui s'appliquent aux CA
2.1.2 Obligations de la RA	Intégré dans les portions du cadre qui s'appliquent aux RA
2.1.3 Obligations du souscripteur	4.1.2, 4.4, 4.5, 4.5.1, 4.6.5, 4.7.5, 4.8.1, 4.8.5, 4.9.1, 4.9.2, 4.9.13, 4.9.15, 5., 6., 9.6.3, 9.9
2.1.4 Obligations du consommateur d'assertions	4.5, 4.5.2, 4.9.6, 5., 6., 9.6.4, 9.9
2.1.5 Obligations du dépositaire	2., 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7
2.2 Responsabilité	9.6, 9.7, 9.8, 9.9
2.2.1 Responsabilité de la CA	9.6.1, 9.7., 9.8, 9.9
2.2.2 Responsabilité de la RA	9.6.2, 9.7, 9.8, 9.9
2.3 Responsabilité financière	9.2
2.3.1 Indemnisation par les consommateurs d'assertions	9.9
2.3.2 Relations fiduciaires	9.7
2.4 Interprétation et mise en application	9.16
2.4.1 Élection de juridiction	9.14, 9.15
2.4.2 Réduction, survivance, fusion, notification	9.10.3, 9.11, 9.16.1,9.16.3
2.4.3 Procédures de résolution de conflit	9.13, 9.16.4
2.5 Redevances	9.1
2.5.1 Redevances de production ou renouvellement de certificat	9.1.1
2.5.2 Redevances d'accès au certificat	9.1.2
2.5.3 Redevances d'accès aux informations de révocation ou d'état	9.1.3
2.5.4 Redevances pour d'autres services (informations de politique)	9.1.4
2.5.5 Politique de refinancement	9.1.5
2.6 Publication et dépôt	2.
2.6.1 Publication des informations de CA	2.2, 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7
2.6.2 Fréquence de publication	2.3
2.6.3 Contrôle d'accès	2.4
2.6.4 Répertoires	2.1
2.7 Audit de conformité	8.
2.7.1 Fréquence de l'audit de conformité de l'entité	8.1
2.7.2 Identité/qualifications de l'auditeur	8.2
2.7.3 Relations de l'auditeur et de l'objet de l'audit	8.3

2.7.4 Sujets couverts par l'audit	8.4
2.7.5 Actions prise suite à des déficiences	8.5
2.7.6 Communications des résultats	8.6
2.8 Confidentialité	9.3, 9.4
2.8.1 Types d'informations à garder confidentielles	9.3.1, 9.4.2
2.8.2 Types d'information non considérées confidentielles	9.3.2, 9.4.3
2.8.3 Divulgation des informations de révocation/suspension	9.3.1, 9.3.2, 9.3.3, 9.4.2, 9.4.3, 9.4.4
2.8.4 Communication aux autorités officielles	9.3.3, 9.4.6
2.8.5 Communication au titre de la découverte civile	9.3.3, 9.4.6
2.8.6 Divulgation sur demande du propriétaire	9.3.3, 9.4.7
2.8.7 Autres circonstances de livraison des informations	9.3.3, 9.4.7
2.9 Droits de propriété intellectuelle	9.5
3. Identification et authentification	3.
3.1 Enregistrement initial	3.1, 3.2
3.1.1 Type de noms	3.1.1
3.1.2 Besoin que les noms soient significatifs	3.1.2, 3.1.3
3.1.3 Règles d'interprétation des diverses formes de nom	3.1.4
3.1.4 Unicité des noms	3.1.5
3.1.5 Procédure de résolution de conflit de revendication de nom	3.1.6
3.1.6 Reconnaissance, authentification, et rôle des marques	3.1.6
3.1.7 Méthode de preuve de possession de clé privée	3.2.1
3.1.8 Authentification d'une identité d'organisation	3.2.2
3.1.9 Authentification d'identité individuelle	3.2.3
3.2 Changement de clé de routine	3.3.1, 4.6, 4.7
3.3 Changement de clé après révocation	3.3.2
3.4 Demande de révocation	3.4
4. Exigences de fonctionnement	4., 5.
4.1 Demande de certificat	4.1, 4.2, 4.6, 4.7
4.2 Production de certificat	4.2, 4.3, 4.4.3, 4.6, 4.7, 4.8.4, 4.8.6, 4.8.7
4.3 Acceptation de certificat	4.3.2, 4.4, 4.6, 4.7, 4.8.4-4.8.7
4.4 Suspension et révocation de certificat	4.8, 4.9
4.4.1 Circonstances de révocation	4.8.1, 4.9.1
4.4.2 Qui peut demander la révocation	4.8.2, 4.9.2
4.4.3 Procédure de demande de révocation	4.8.3-4.8.7, 4.9.3
4.4.4 Période de grâce de demande de révocation	4.9.4
4.4.5 Circonstances de la suspension	4.9.13
4.4.6 Qui peut demander la suspension	4.9.14
4.4.7 Procédure de la demande de suspension	4.9.15
4.4.8 Limites de la période de suspension	4.9.16
4.4.9 Fréquence de production de CRL (si applicable)	4.9.7, 4.9.8, 4.10
4.4.10 Exigences de vérification de CRL	4.9.6, 4.10
4.4.11 Disponibilité de vérification en ligne de révocation/état	4.9.9, 4.10
4.4.12 Exigences de vérification en ligne de révocation	4.9.6, 4.9.10, 4.10
4.4.13 Autres formes d'annonce de révocation	4.9.11, 4.10
4.4.14 Exigences de vérification des autres formes d'annonce de révocation	4.9.6, 4.9.11, 4.10
4.4.15 Exigences spéciales du changement de clés sur compromission	4.9.12
4.5 Procédures d'audit de sécurité	5.4
4.5.1 Types d'événements enregistrés	5.4.1
4.5.2 Fréquence de traitement du journal d'audit	5.4.2
4.5.3 Période de rétention du journal d'audit	5.4.3
4.5.4 Protection du journal d'audit	5.4.4
4.5.5 Procédures de sauvegarde du journal d'audit	5.4.5
4.5.6 Système de collecte du journal d'audit (interne ou externe)	5.4.6
4.5.7 Notification au sujet cause d'événement	5.4.7
4.5.8 Évaluation des vulnérabilités	5.4.8
4.6 Archivage des enregistrements	5.5
4.6.1 Types d'enregistrements archivés	5.5.1
4.6.2 Période de rétention des archives	5.5.2
4.6.3 Protection des archives	5.5.3
4.6.4 Procédures de sauvegarde des archives	5.5.4
4.6.5 Exigences d'horodatage des enregistrements	5.5.5
4.6.6 Système de collecte des archives (interne ou externe)	5.5.6
4.6.6 Procédures pour obtenir et vérifier les informations d'archive	5.5.7

4.7 Changement de clés	5.6
4.8 Récupération sur compromission et désastre	5.7, 5.7.1
4.8.1 Corruption des ressources informatiques	5.7.2
4.8.2 Révocation de la clé publique de l'entité	4.9.7, 4.9.9, 4.9.11
4.8.3 Compromission de la clé de l'entité	5.7.3
4.8.4 Sécurisation des facilité après désastre naturel ou autre	5.7.4
4.9 Terminaison de CA	5.8
5. Contrôles de sécurité physique, procédurale, et personnelle	5.
5.1 Contrôles physiques	5.1
5.1.1 Localisation et construction du site	5.1.1
5.1.2 Accès physique	5.1.2
5.1.3 Alimentation en énergie et air conditionné	5.1.3
5.1.4 Dégâts des eaux	5.1.4
5.1.5 Prévention et protection d'incendie	5.1.5
5.1.6 Stockage des supports	5.1.6
5.1.7 Élimination des déchets	5.1.7
5.1.8 Sauvegarde hors site	5.1.8
5.2 Contrôles procéduraux	5.2
5.2.1 Rôles de confiance	5.2.1, 5.2.4
5.2.2 Nombre de personnes requis par tâche	5.2.2, 5.2.4
5.2.3 Identification et authentification pour chaque rôle	5.2.3
5.3 Contrôles des personnes	5.3
5.3.1 Exigences de cursus, qualifications, expérience, et habilitation	5.3.1
5.3.2 Procédures de vérification du cursus	5.3.2
5.3.3 Exigences de formation	5.3.3
5.3.4 Fréquence et exigences de formation continue	5.3.4
5.3.5 Fréquence et séquence de rotation des postes	5.3.5
5.3.6 Sanctions des actions non autorisées	5.3.6
5.3.7 Exigences pour le personnel contractuel	5.3.7
5.3.8 Documentation fournie au personnel	5.3.8
6. Contrôles de sécurité technique	6.
6.1 Génération et installation de la paire de clés	6.1
6.1.1 Génération de la paire de clés	6.1.1
6.1.2 Livraison de la clé privée à l'entité	6.1.2
6.1.3 Livraison de la clé publique au producteur de certificat	6.1.3
6.1.4 Livraison de la clé publique de la CA aux utilisateurs	6.1.4
6.1.5 Tailles de clés	6.1.5
6.1.6 Génération des paramètres de clé publique	6.1.6
6.1.7 Vérification de la qualité des paramètres	6.1.6
6.1.8 Génération de clé de matériel/logiciel	6.1.1
6.1.9 Usage de la clé (selon le champ Usage de clé de X.509 v3)	6.1.9
6.2 Protection de la clé privée	6.2
6.2.1 Normes du module cryptographique	6.2.1
6.2.2 Contrôle multi personnes de clé privée (n parmi m)	6.2.2
6.2.3 Tiers de confiance de clé privée	6.2.3
6.2.4 Sauvegarde de clé privée	6.2.4
6.2.5 Archivage de clé privée	6.2.5
6.2.6 Entrée de la clé privée dans le module cryptographique	6.2.6, 6.2.7
6.2.7 Méthode d'activation de la clé privée	6.2.8
6.2.8 Méthode de désactivation de la clé privée	6.2.9
6.2.9 Méthode de destruction de la clé privée	6.2.10
6.3 Autres aspects de gestion de la paire de clés	6.3
6.3.1 Archivage de la clé publique	6.3.1
6.3.2 Périodes d'usage des clés publique et privée	6.3.2
6.4 Données d'activation	6.4
6.4.1 Génération et installation des données d'activation	6.4.1
6.4.2 Protection des données d'activation	6.4.2
6.4.3 Autres aspects des données d'activation	6.4.3
6.5 Contrôles de sécurité informatique	6.5
6.5.1 Exigences techniques spécifiques de sécurité informatique	6.5.1
6.5.2 Classement de la sécurité informatique	6.5.2
6.6 Contrôles techniques du cycle de vie	6.6
6.6.1 Contrôles du développement du système	6.6.1

6.6.2 Contrôles de la gestion de la sécurité	6.6.2
6.6.3 Contrôles de la sécurité du cycle de vie	6.6.3
6.7 Contrôles de la sécurité du réseau	6.7
6.8 Contrôles de l'ingénierie du module cryptographique	6.2.1, 6.2, 6.2.1, 6.2.11
7. Profils de certificat et de CRL	7.
7.1 Profil de certificat	7.1
7.1.1 Numéros de version	7.1.1
7.1.2 Extensions de certificat	7.1.2
7.1.3 Identifiants d'objet d'algorithme	7.1.3
7.1.4 Formes des noms	7.1.4
7.1.5 Contraintes sur les noms	7.1.5
7.1.6 Identifiant d'objet de politique de certificat	7.1.6
7.1.7 Usage de l'extension de contraintes de politique	7.1.7
7.1.8 Syntaxe et sémantique des qualificatifs de politique	7.1.8
7.1.9 Sémantique du traitement de l'extension politique de certificat	7.1.9
7.2 Profil de CRL	7.2
7.2.1 Numéros de version	7.2.1
7.2.2 CRL et extensions d'entrées de CRL	7.2.1
8. Administration de la spécification	N/A
8.1 Procédures de changement de spécification	9.12
8.2 Politiques de publication et de notification	2.2, 2.3
8.3 Procédures d'approbation de CPS	1.5.4

La matrice qui suit donne les paragraphes du nouveau cadre et les paragraphes de la RFC 2527 auxquels correspondent les intitulés du nouveau cadre.

Section de la nouvelle RFC	**Section originale de la RFC 2527**
1. Introduction	1.
1.1 Généralités	1.1
1.2 Nom et identification du document	1.2
1.3 Participants à la PKI	1.3
1.3.1 Autorités de certification	1.3.1
1.3.2 Autorités d'enregistrement	1.3.2
1.3.3 Souscripteurs	1.3.3
1.3.4 Consommateurs d'assertions	1.3.3
1.3.5 Autres participants	N/A
1.4 Usage du certificat	1.3.4
1.4.1 Utilisation appropriée du certificat	1.3.4
1.4.2 Utilisations interdites du certificat	1.3.41.5 Administration de la politique 1.4
1.5.1 Organisation qui gère le document	1.4.1
1.5.2 Personne à contacter	1.4.2
1.5.3 Personne qui détermine que la CPS convient pour la politique	1.4.3
1.5.4 Procédures d'approbation de CPS	8.3
1.6 Définitions et acronymes	N/A
2. Responsabilité de la publication et du répertoire	2.1.5, 2.6
2.1 Répertoires	2.6.4
2.2 Publication des informations de certification	2.6.1, 8.2
2.3 Moment ou fréquence de la publication	2.6.2, 8.2
2.4 Contrôle de l'accès aux répertoires	2.6.3
3. Identification et authentification	3.
3.1 Désignation	3.1
3.1.1 Type des noms	3.1.1
3.1.2 Besoin que les noms aient une signification	3.1.2
3.1.3 Anonymat ou pseudonyme des souscripteurs	3.1.2
3.1.4 Règles d'interprétation des diverses formes de noms	3.1.3
3.1.5 Unicité des noms	3.1.4
3.1.6 Reconnaissance, authentification, et rôle des marques	3.1.5, 3.1.6
3.2 Validation d'identité initiale	3.1
3.2.1 Méthode de preuve de possession de clé privée	3.1.7
3.2.2 Authentification d'identité d'organisation	3.1.8
3.2.3 Authentification d'identité individuelle	3.1.9
3.2.4 Informations de souscripteur non vérifiées	N/A

3.2.5 Validation d'autorité	3.1.9
3.2.6 Critères d'interopération	4.1
3.3 Identification et authentification des demandes de changement de clé	3.2, 3.3
3.3.1 Identification et authentification des changements de clé de routine	3.2
3.3.2 Identification et authentification de changement de clé sur révocation	3.3
3.4 Identification et authentification des demandes de révocation	3.4
4. Exigences de fonctionnement sur le cycle de vie du certificat	4.
4.1 Demande de certificat	4.1
4.1.1 Qui peut soumettre une demande de certificat	4.1
4.1.2 Processus et responsabilité des engagements	2.1.3, 4.1
4.2 Traitement des demandes de certificat	4.1, 4.2
4.2.1 Exécution des fonctions d'identification et d'authentification	4.1, 4.2
4.2.2 Approbation ou rejet des demandes de certificat	4.1, 4.2
4.2.3 Délai de traitement des demandes de certificat	4.1, 4.2
4.3 Production du certificat	4.2
4.3.1 Actions de la CA durant la production du certificat	4.2
4.3.2 Notification au souscripteur de la production du certificat par la CA	4.2, 4.3
4.4 Acceptation du certificat	2.1.3, 4.3
4.4.1 Conduite constituant une acceptation de certificat	4.3
4.4.2 Publication du certificat par la CA	2.1.5, 2.6.1, 4.3
4.4.3 Notification de la production de certificat par la CA aux autres entités	2.1.5, 2.6.1, 4.2, 4.3
4.5 Utilisation de la paire de clés et du certificat	1.3.4, 2.1.3, 2.1.4
4.5.1 Utilisation de la paire de clés et du certificat par le souscripteur	1.3.4, 2.1.3
4.5.2 Utilisation de la paire de clés et du certificat par le consommateur d'assertions	1.3.4, 2.1.4
4.6 Renouvellement de certificat	3.2, 4.1, 4.2, 4.3
4.6.1 Circonstances du renouvellement de certificat	3.2, 4.1
4.6.2 Qui peut demander le renouvellement	3.2, 4.1
4.6.3 Traitement des demandes de renouvellement de certificat	3.2, 4.1, 4.2
4.6.4 Notification de la production du nouveau certificat au souscripteur	3.2, 4.2, 4.3
4.6.5 Conduite constituant l'acceptation du renouvellement de certificat	2.1.3, 3.2, 4.3
4.6.6 Publication du renouvellement de certificat par la CA	2.1.5, 2.6.1, 3.2, 4.3
4.6.7 Notification de la production du certificat aux autres entités par la CA	2.1.5, 2.6.1, 3.2, 4.2, 4.3
4.7 Changement de clés de certificat	3.2, 4.1, 4.2, 4.3
4.7.1 Circonstances du changement de clés de certificat	3.2, 4.1
4.7.2 Qui peut demander la certification d'une nouvelle clé publique	3.2, 4.1
4.7.3 Traitement des demandes de certificat de changement de clés	3.2, 4.1, 4.2
4.7.4 Notification de la production du nouveau certificat au souscripteur	3.2, 4.2, 4.3
4.7.5 Conduites constituant l'acceptation d'un certificat de changement de clé	2.1.3, 3.2, 4.3
4.7.6 Publication du certificat de changement de clé par la CA	2.1.5, 2.6.1, 3.2, 4.3
4.7.7 Notification de la production du certificat aux autres entités pas la CA	2.1.5, 2.6.1, 3.2, 4.2, 4.3
4.8 Modification de certificat	4.4
4.8.1 Circonstances de modification de certificat	2.1.3, 4.4.1
4.8.2 Qui peut demander la modification de certificat	4.4.2
4.8.3 Traitement des demandes de modification de certificat	4.4.3
4.8.4 Notification de la production du nouveau certificat au souscripteur	4.2, 4.3, 4.4.3
4.8.5 Conduites constituant l'acceptation d'un certificat modifié	2.1.3, 4.3, 4.4.3
4.8.6 Publication du certificat modifié par la CA	2.1.5, 2.6.1, 4.2, 4.3, 4.4.3
4.8.7 Notification de la production du certificat aux autres entités par la CA	2.1.5, 2.6.1, 4.2, 4.3, 4.4.3
4.9 Révocation et suspension du certificat	4.4
4.9.1 Circonstances de révocation	2.1.3, 4.4.1
4.9.2 Qui peut demander la révocation	4.4.2
4.9.3 Procédure de la demande de révocation	2.1.3, 4.4.3
4.9.4 Période de grâce de la demande de révocation	4.4.4
4.9.5 Délai dans lequel la CA doit traiter la demande de révocation	N/A
4.9.6 Exigences de vérification de révocation pour le consommateur d'assertion	2.1.4, 4.4.10, 4.4.12, 4.4.14
4.9.7 Fréquence de production de CRL	4.4.9, 4.8.3
4.9.8 Latence maximum des CRL	4.4.9
4.9.9 Disponibilité en ligne de la vérification d'état/révocation	4.4.11, 4.8.3
4.9.10 Exigences de la vérification en ligne de révocation	4.4.12
4.9.11 Autres formes d'annonce de révocation disponibles	4.4.13, 4.4.14, 4.8.3
4.9.12 Exigences spéciales du changement de clé sur compromission	4.4.15
4.9.13 Circonstances de la suspension	2.1.3, 4.4.5
4.9.14 Qui peut demander la suspension	4.4.6

4.9.15 Procédure de la demande de suspension	2.1.3, 4.4.7
4.9.16 Limites de la période de suspension	4.4.8
4.10 Services d'état de certificat	4.4.9-4.4.14
4.10.1 Caractéristiques de fonctionnement	4.4.9, 4.4.11, 4.4.13
4.10.2 Disponibilité du service	4.4.9, 4.4.11, 4.4.13
4.10.3 Dispositifs opérationnels	4.4.9, 4.4.11, 4.4.13
4.11 Fin d'abonnement	N/A
4.12 Mise en dépôt et récupération de clé	6.2.3
4.12.1 Politique et pratiques de mise en dépôt et récupération de clé	6.2.3
4.12.2 Politique et pratiques d'encapsulation de clé de session et de récupération	6.2.3
5. Contrôle des facilités, de la gestion et du fonctionnement	2.1.3, 2.1.4, 4., 5.
5.1 Contrôles physiques	5.1
5.1.1 Localisation et construction du site	5.1.1
5.1.2 Accès physique	5.1.2
5.1.3 Alimentation électrique et air conditionné	5.1.3
5.1.4 Dégâts des eaux	5.1.4
5.1.5 Prévention et protection contre l'incendie	5.1.5
5.1.6 Stockage des supports	5.1.6
5.1.7 Élimination des déchets	5.1.7
5.1.8 Sauvegarde hors site	5.1.8
5.2 Contrôles procéduraux	5.2
5.2.1 Rôles de confiance	5.2.1
5.2.2 Nombre de personnes requis par tâche	5.2.2
5.2.3 Identification et authentification pour chaque rôle	5.2.3
5.2.4 Rôles exigeant une séparation des tâches	5.2.1, 5.2.2
5.3 Contrôles sur le personnel	5.3
5.3.1 Exigences de qualifications, d'expérience, et d'habilitation	5.3.1
5.3.2 Procédures de vérification des cursus	5.3.2
5.3.3 Exigences de formation	5.3.3
5.3.4 Fréquence et exigences de formation continue	5.3.4
5.3.5 Fréquence et séquence de rotation des tâches	5.3.5
5.3.6 Sanctions des actions non autorisées	5.3.6
5.3.7 Exigences pour les contractuels indépendants	5.3.7
5.3.8 Documentation fournie au personnel	5.3.8
5.4 Procédures d'enregistrement d'audit	4.5
5.4.1 Types d'événements enregistrés	4.5.1
5.4.2 Fréquence de traitement du journal d'audit	4.5.2
5.4.3 Période de rétention du journal d'audit	4.5.3
5.4.4 Protection du journal d'audit	4.5.4
5.4.5 Procédures de sauvegarde du journal d'audit	4.5.5
5.4.6 Système de collecte des données d'audit (interne ou externe)	4.5.6
5.4.7 Notification à la cause d'un événement	4.5.7
5.4.8 Évaluation des vulnérabilités	4.5.8
5.5 Archivage des enregistrements	4.6
5.5.1 Types d'archivage des enregistrements	4.6.1
5.5.2 Période de rétention des archives	4.6.2
5.5.3 Protection des archives	4.6.3
5.5.4 Procédures de sauvegarde des archives	4.6.4
5.5.5 Exigences d'horodatages des enregistrements	4.6.5
5.5.6 Système de collecte des archives (interne ou externe)	4.6.6
5.5.7 Procédure pou obtenir et vérifier les informations d'archive	4.6.7
5.6 Changement de clé	4.7
5.7 Récupération sur compromission et désastre	4.8
5.7.1 Procédures de traitement d'incident et de compromission	4.8
5.7.2 Corruption des ressources informatiques, logicielles et/ou données	4.8.1
5.7.3 Procédures en cas de compromission de la clé privée de l'entité	4.8.3
5.7.4 Capacités de poursuite d'activité après désastre	4.8.4
5.8 Terminaison de CA ou RA	4.9
6. Contrôles de sécurité technique	2.1.3, 2.1.4, 6.
6.1 Génération et installation de paire de clés	6.1
6.1.1 Génération de paire de clés	6.1.1, 6.1.8
6.1.2 Livraison de clé privée au souscripteur	6.1.2
6.1.3 Livraison de clé publique au producteur de certificat	6.1.3

6.1.4 Livraison de clé publique de CA aux consommateurs d'assertions	6.1.4
6.1.5 Tailles de clé	6.1.5
6.1.6 Génération et vérification de la qualité des paramètres de clé publique	6.1.6, 6.1.7
6.1.7 Objet de l'usage de clé (selon le champ Usage de clé de X.509 v3)	6.1.9
6.2 Contrôle de protection de clé privée et d'ingénierie de module cryptographique	6.2, 6.8
6.2.1 Normes et contrôle du module cryptographique	6.2.1, 6.8
6.2.2 Contrôle multi personnes de clé privée (n parmi m)	6.2.2
6.2.3 Tiers de confiance de clé privée	6.2.3
6.2.4 Sauvegarde de clé privée	6.2.4
6.2.5 Archivage de clé privée	6.2.5
6.2.6 Transfert de clé privée dans ou d'un module cryptographique	6.2.6
6.2.7 Mémorisation de clé privée sur un module cryptographique	6.2.6
6.2.8 Méthode d'activation de clé privée	6.2.7
6.2.9 Méthode de désactivation de clé privée	6.2.8
6.2.10 Méthode de destruction de clé privée	6.2.9
6.2.11 Classement du module cryptographique	6.2.1, 6.8
6.3 autres aspects de la gestion de la paire de clés	6.3
6.3.1 Archivage de clé publique	6.3.1
6.3.2 Périodes de fonctionnement de certificat et d'usage de paire de clés	6.3.2
6.4 Données d'activation	6.4
6.4.1 Génération et installation des données d'activation	6.4.1
6.4.2 Protection des données d'activation	6.4.2
6.4.3 Autres aspects des données d'activation	6.4.3
6.5 Contrôles de la sécurité informatique	6.5
6.5.1 Exigences techniques spécifiques de la sécurité informatique	6.5.1
6.5.2 Classement de la sécurité informatique	6.5.2
6.6 Contrôles techniques sur le cycle de vie	6.6
6.6.1 Contrôles sur le développement du système	6.6.1
6.6.2 Contrôles sur la gestion de la sécurité	6.6.2
6.6.3 Contrôles sur la sécurité du cycle de vie	6.6.3
6.7 Contrôles sur la sécurité du réseau	6.7
6.8 Horodatage	N/A
7. Profils de certificat, de CRL, et d'OCSP	7.
7.1 Profils de certificat,	7.1
7.1.1 Numéros de version	7.1.1
7.1.2 Extensions de certificat	7.1.2
7.1.3 Identifiants d'objet d'algorithme	7.1.3
7.1.4 Formes de noms	7.1.4
7.1.5 Contraintes de noms	7.1.5
7.1.6 Identifiants d'objet de politique de certificat	7.1.6
7.1.7 Extensions de contraintes d'usage de politique	7.1.7
7.1.8 Syntaxe et sémantique des qualificatifs de politique	7.1.8
7.1.9 Sémantique du traitement de l'extension critique de politique de certificat	7.1.9
7.2 Profil de CRL	7.2
7.2.1 Numéros de version	7.2.1
7.2.2 CRL et extensions d'entrée de CFL	7.2.1
7.3 Profil d'OCSP	N/A
7.3.1 Numéros de version	N/A
7.3.2 Extensions d'OCSP	N/A
8. Audit de conformité et autres évaluations	2.7
8.1 Fréquence et circonstances d'évaluation	2.7.1
8.2 Identité/qualifications de l'évaluateur	2.7.2
8.3 Relations de l'évaluateur avec l'entité évaluée	2.7.3
8.4 Sujets couverts par l'évaluation	2.7.4
8.5 Actions prises suite à une déficience	2.7.5
8.6 Communications des résultats	2.7.6
9. Autres sujets d'affaire et juridiques	2.
9.1 Redevances	2.5
9.1.1 Redevances de production ou renouvellement de certificat	2.5.1
9.1.2 Redevances d'accès au certificat	2.5.2
9.1.3 Redevances d'accès aux informations de révocation/état	2.5.3
9.1.4 Redevances pour d'autres services	2.5.4
9.1.5 Politique de refinancement	2.5.5

9.2 Responsabilité financière	2.3
9.2.1 Couverture des assurances	2.3
9.2.2 Autres biens	2.3
9.2.3 Assurance ou garantie pour les entités d'extrémité	2.3
9.3 Confidentialité des informations d'affaires	2.8
9.3.1 Portée des informations confidentielles	2.8.1, 2.8.3
9.3.2 Informations non considérées comme confidentielles	2.8.2, 2.8.3
9.3.3 Responsabilité de protection des informations confidentielles	2.8, 2.8.3-2.8.7
9.4 Confidentialité des informations personnelles	2.8
9.4.1 Plan de confidentialité	N/A
9.4.2 Informations traitées comme privées	2.8.1, 2.8.3
9.4.3 Information non réputées privées	2.8.2, 2.8.3
9.4.4 Responsabilité de la protection des informations privées	2.8, 2.8.1, 2.8.3
9.4.5 Notification et consentement à l'utilisation des informations privées	N/A
9.4.6 Divulgation suite à poursuites judiciaires ou administratives	2.8.4-2.8.5
9.4.7 Autres circonstances de divulgation des informations	2.8.6-2.8.7
9.5 Droits de propriété intellectuelle	2.9
9.6 Représentations et garanties	2.2
9.6.1 Représentations et garanties de la CA	2.2.1
9.6.2 Représentations et garanties de la RA	2.2.2
9.6.3 Représentations et garanties du souscripteur	2.1.3
9.6.4 Représentations et garanties du consommateur d'assertions	2.1.4
9.6.5 Représentations et garanties des autres participants	N/A
9.7 Renonciation à garanties	2.2, 2.3.2
9.8 Limitations de responsabilité	2.2
9.9 Indemnités	2.1.3, 2.1.4, 2.2, 2.3.1
9.10 Terme et terminaison	N/A
9.10.1 Terme	N/A
9.10.2 Terminaison	N/A
9.10.3 Effet de la terminaison et survivances	N/A
9.11 Notifications individuelles et communications avec les participants	2.4.2
9.12 Amendements	8.1
9.12.1 Procédure des amendements	8.1
9.12.2 Mécanisme et période de notification	8.1
9.12.3 Circonstances dans lesquelles un OID doit être changé	8.1
9.13 Dispositions sur la résolution des conflits	2.4.3
9.14 Élection de juridiction	2.4.1
9.15 Conformité à la loi applicable	2.4.1
9.16 Dispositions diverses	2.4
9.16.1 Accord complet	2.4.2
9.16.2 Affectation	N/A
9.16.3 Réduction	2.4.2
9.16.4 Mise en application (frais juridiques et renonciation de droits)	2.4.3
9.17 Autres dispositions	N/A

8. Remerciements

Le développement du document antérieur (RFC2527) a été soutenu par le comité d'autorité de gestion de politique (PMA, *Policy Management Authority*) du Gouvernement du Canada , L'Agence Nationale de Sécurité (NSA), l'Institut National des normes et technologies (NIST), et le groupe de travail Accréditation du comité de sécurité de l'information de l'Association américaine des avocats .

Cet effort de révision est largement le résultat de l'inspiration constante de Michael Baum. Michael Power, Mike Jenkins, et Alice Sturgeon ont aussi produit plusieurs contributions.

9. Références

[ABA1] American Bar Association, "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities et Secure Electronic Commerce", 1996.

[ABA2] American Bar Association, "PKI Assessment Guidelines, v0.30", projet public pour commentaire, juin 2001.

[BAU1] Michael. S. Baum, "Federal Certification Authority Liability et Policy", NIST-GCR-94-654, juin 1994, disponible à http://www.verisign.com/repository/pubs/index.html .

[ETS] European Telecommunications Standards Institute, "Policy Requirements for Certification Authorities Issuing Qualified Certificates," ETSI TS 101 456, Version 1.1.1, décembre 2000.

[GOC] Government of Canada PKI Policy Management Authority, "Digital Signature et Confidentiality Certificate Policies for the Government of Canada Public Key Infrastructure, v.3.02", avril 1999.

[IDT] Identrus, LLC, "Identrus Identity Certificate Policy" IP-IPC Version 1.7, mars 2001.

[ISO1] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework," édition 1997. (en attendant la publication de l'édition 2000).

[RFC1422] S. Kent, "Amélioration de la confidentialité pour la messagerie électronique Internet : Partie II – Gestion de clés fondée sur le certificat", février 1993. *(Historique)*

[RFC2527] S. Chokhani, W. Ford, "Cadre pour la politique de certificats d'infrastructure de clés publiques X.509 sur Internet et pour les pratiques de certification", mars 1999. (*Obsolète, voir* RFC3647) *(Information)*

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

10. Notes

(1) Une copie papier des Lignes directrices pour les signatures numériques de l'ABA peut être achetée auprès de l'ABA. Voir le formulaire de commande à http://www.abanet.com. La DSG peut aussi être téléchargée sans frais sur le site de l'ABA à http://www.abanet.org/scitech/ec/isc/digital_signature.html .

(2) Un projet des lignes directrices pour l'évaluation de PKI peut être téléchargé sans frais du site de la Toile de l'ABA à : http://www.abanet.org/scitech/ec/isc/pag/pag.html .

(3) Le terme "significatif" signifie que la forme du nom a une sémantique généralement comprise comme déterminant l'identité d'une personne et/ou d'une organisation. Les noms des répertoires et les noms de la RFC 822 peuvent être plus ou moins significatifs.

(4) Le sujet peut n'avoir pas besoin de prouver à la CA qu'il est en possession de la clé privée correspondant à la clé publique enregistrée si la CA génère la paire de clés du sujet au nom du sujet.

(5) Des exemples de moyens d'identifier et d'authentifier les individus incluent les moyens biométriques (comme l'empreinte du pouce, l'empreinte des dix doigts, une photographie du visage, de la paume de la main, ou de la rétine) un permis de conduire, une carte de crédit, l'insigne d'une société, et l'insigne d'un fonctionnaire du gouvernement.

(6) La "modification" d'un certificat ne se réfère pas à effectuer un changement à un certificat existant, car cela empêcherait la vérification des signatures numériques sur le certificat et causerait l'invalidation du certificat. Le concept de "modification" se réfère plutôt à une situation où les informations auxquelles on se réfère dans le certificat ont changé ou devraient être changées, et la CA produit un nouveau certificat contenant les informations modifiées. Un exemple est celui d'un souscripteur qui change de nom, ce qui nécessiterait la production d'un nouveau certificat contenant le nouveau nom.

(7) La règle n parmi m permet à une clé privée d'être partagée en m parts. Les m parts peuvent être données à m individus différents. Toutes les n parts parmi les m parts peuvent être utilisées pour reconstituer pleinement la clé privée, mais n'avoir que n-1 parts ne donne aucune information sur la clé privée.

(8) Une clé privée peut être confiée à un tiers de confiance, sauvegardée, ou archivée. Chacune de ces fonctions a un objet différent. Donc, une clé privée peut passer par n'importe quel sous ensemble de ces fonctions selon les exigences. L'objet du dépôt chez un tiers de confiance est de permettre qu'un tiers (comme une organisation ou un officier public) obtienne la clé sans la coopération de l'abonné. L'objet de la sauvegarde est de permettre au souscripteur de reconstituer la clé en cas de destruction ou corruption de la clé, pour les besoins de la continuité des affaires. L'objet de l'archivage

est d'assurer la réutilisation de la clé privée à l'avenir, par exemple, pour déchiffrer un document.

(9) WebTrust se réfère au "programme WebTrust pour les autorités de certification" de l'institut américain des comptables publics certifiés (American Institute of Certified Public Accountants, Inc.) et de l'institut canadien des comptables agréées (Canadian Institute of Chartered Accountants).

(10) Voir < http://www.aicpa.org >.

(11) Tous les éléments suivants ou certains d'entre eux peuvent être différents pour les divers types d'entités, c'est-à-dire, CA, RA, et entités d'extrémité.

11. Liste des acronymes

ABA *(American Bar Association)* Association des avocats des États Unis d'Amérique
CA *(Certification Authority)* Autorité de certification
CP *(Certificate Policy)* politique de certificat
CPS *(Certification Practice Statement)* déclaration de pratique de certification
CRL *(Certificate Revocation List)* liste de révocation de certificats
DAM *(Draft Amendment)* projet d'amendement
FIPS *(Federal Information Processing Standard)* normé fédérale de traitement de l'information
I&A *(Identification et authentification)* identification et authentification
CEI *(Comité électrotechnique international)* International Electrotechnical Commission
IETF *(Internet Engineering Task Force)* équipe d'ingénierie de l'Internet
IP *(Internet Protocol)* Protocole Internet
ISO *(International Standard Organization)* Organisation internationale de normalisation
UIT *(Union internationale des télécommunications)* International Telecommunications Union (ITU)
NIST *(National Institute of Standards et Technology)* Institut national des normes et technologies
OID *(Object Identifier)* identifiant d'objet
PIN *(Personal Identification Number)* numéro d'identification personnel
PKI *(Public Key Infrastructure)* infrastructure de clé publique
PKIX *(Public Key Infrastructure X.509)* infrastructure de clé publique X.509 (groupe de travail de l'IETF)
RA *(Registration Authority)* autorité d'enregistrement
RFC *(Request For Comment)* Appel à commentaires
URL *(Uniform Resource Locator)* localisateur de ressource universel
US *(United States)* États-Unis d'Amérique

12. Adresse des auteurs

Santosh Chokhani
Orion Security Solutions, Inc.
3410 N. Buchanan Street
Arlington, VA 22207
téléphone : (703) 237-4621
mél : chokhani@orionsec.com

Warwick Ford
VeriSign, Inc.
6 Ellery Square
Cambridge, MA 02138
téléphone : (617) 642-0139
mél : wford@verisign.com

Randy V. Sabett, J.D., CISSP
Cooley Godward LLP
One Freedom Square, Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656
téléphone : (703) 456-8137
mél : rsabett@cooley.com

Charles (Chas) R. Merrill
McCarter & English, LLP
Four Gateway Center
100 Mulberry Street
Newark, New Jersey 07101-0652
téléphone : (973) 622-4444
mél : cmerrill@mccarter.com

Stephen S. Wu
Infoliance, Inc.
800 West El Camino Real
Suite 180
Mountain View, CA 94040
téléphone : (650) 917-8045
mél : swu@infoliance.com

13. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d’édition des RFC est actuellement fourni par l’Internet Society.