rfc3647

Framework de stratégie de certificat et de pratiques de certification

Introduction

En général, un certificat à clé publique lie une clé publique maintenue par une entité (telle qu'une personne, une organisation, compte, périphérique, ou site) à un jeu d'informations qui identifient l'entité associée avec l'utilisation de la clé privée correspondante. Dans beaucoup de cas impliquant des certificats d'identité, cette entité est connue comme le "subject" ou "subscriber" du certificat. 2 exceptions cependant, incluant les périphérique (dans lequel le souscripteur est généralement l'organisation contrôlant le périphérique) et les certificats anonymes (dans lequel l'identité de l'individu ou de l'organisation n'est pas disponible depuis le certificat lui-même). D'autres types de certificats lient les clés publiques aux attributs d'une entité autre que l'identité de l'entité, tel qu'un rôle, un titre, ou des informations de solvabilité.

Un certificat est utilisé par un utilisateur de certificat ou un tiers de confiance qui a besoin d'utiliser, et compte sur la précision de, le lien entre la clé publique du sujet distribué via ce certificat et l'identité et/ou d'autres attributs du sujet contenu dans ce certificat. Un tiers de confiance est fréquemment une entité qui vérifie la signature numérique du sujet du certificat où la signature numérique est associée avec un mail, document électronique, ou autre donnée. D'autres exemples de tiers de confiance peut inclure un émetteur de mail chiffré à un souscripteur, un utilisateur d'un navigateur web vérifiant un certificat serveur durant une session SSL, et une entité opérant un serveur qui contrôle l'accès aux informations online en utilisant des certificats client comme mécanisme de contrôle d'accès. En résumé, un tiers de confiance est une entité qui utilise une clé publique dans un certificat (pour vérification de signature et/ou chiffrement). Le degré auquel le tiers de confiance peut faire confiance à la liaison embarquée dans un certificat dépend de nombreux facteurs. Ces facteurs peuvent inclure les pratiques suivies par l'autorité de certification en authentifiant le sujet ; la stratégie de la CA, les procédures, et les contrôles de sécurité. Le scope de la responsabilité du souscripteur (par exemple, en protégeant la clé privée) ; et les responsabilités statué et les termes et conditions de responsabilité de la CA.

Un certificat X.509 version 3 peut contenir un champ déclarant qu'une ou plusieurs stratégies de certificat spécifiques s'appliquent à ce certificat. En accord avec X.509, une stratégie de certificat (CP) est "un jeu de règles nommés qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou classe d'applications avec des pré-requis de sécurité communs". Un CP peut être utilisé par un tiers de confiance pour aider à décider si un certificat est suffisamment digne de confiance et par ailleurs approprié pour une application particulière. Le concept CP est un prolongement du concept de déclaration de stratégie développé pour Internet Privacy Enhanced Mail.

Une description plus détaillée des pratiques suivies par une CA en émettant et gérant des certificats peut être contenu dans une déclaration de pratique de certification (CPS) publié par ou référencé par la CA. En accord avec American Bar Association Information Security Committee's Digital Signature Guidelines (DSG) et l'Information Security Committee's PKI Assessment Guidelines (PAG), "un CPS est une déclaration des utilisations qu'une autorité de certification emploie pour émettre des certificats". En général, les CPS décrivent également des pratiques liées à tous les services de cycle de vie des certificats (ex : émission, gestion, révocation, renouvellement, etc), et les CPS fournissent des détails concernant d'autres question d'affaires, juridiques et techniques. Les termes contenus dans un CP ou CPS peuvent ou non être obligatoire pour les participants d'une PKI comme un contrat. Un CP ou CPS peut lui-même prétendre être un contrat. Plus communément, cependant, un agrément peut incorporer un CP ou CPS par référence et ainsi tenter de lier les parties de l'agrément à partie ou tous ses termes. Par exemple, certaines PKI peuvent utiliser un CP ou (plus communément) un CPS qui est incorporé par référence dans l'agrément entre un souscripteur et une CA ou RA (appelé un agrément de souscripteur) ou l'agrément entre un tiers de confiance et une CA (appelé un agrément de tiers de confiance ou RPA). Dans d'autres cas, cependant, un CP ou CPS n'a pas de signification contractuelle du tout. Une PKI peut définir ces CP ou CPS comme étant strictement informationels ou des documents d'information.

But

Le but de ce document est double. D'abord, le document explique les concepts d'un CP ou d'un CPS, décris les différences entre ces 2 concepts, et décris leur relation au souscripteur et agréments de tiers de confiance. Ensuite, ce document présente un framework pour assister les rédacteurs et utilisateurs de stratégie de certificat ou CPS en définissant et comprenant ces documents. En particulier, le framework identifie les éléments qui peuvent être nécessaire à considérer en formulant un CP ou CPS. Le but n'est pas de définir de stratégie de certificat particulière ou CPS.

Périmètre

Le périmètre de ce document est limité à la discussion des éléments qui peuvent être couverts dans un CP (comme définis dans X.509) ou CPS (comme définis dans DSG et PAG). En particulier, ce document décris les types d'information qui devraient être considérés pour les inclure dans un CP ou CPS. Bien que le framework présenté généralement assume l'utilisation de certificat X.509v3 pour fournir l'assurance d'identité, il n'est pas prévus qu'il soit restreint à l'utilisation de ce format de certificat. À la place, il est prévus que ce framework soit adaptable à d'autres formats de certificat et certificats fournissant des assurance autre que l'identité qui peuvent entrer en utilisation.

Le scope ne s'étend pas à la définition des stratégies de certificat (tels que les stratégies de sécurité des organisation, stratégie de sécurité des systèmes, ou stratégie de labelisation des données). De plus, ce document ne définis pas de CP ou CPS spécifiue. En outre, en présentant un framework, ce document devrait être vu et utilisé comme un outil flexible présentant des éléments qui devraient être considérés comme un intérêt particulier pour les CP ou CPS, et pas comme une formue rigide pour produire des CP ou CPS.

Ce document assume que le lecteur est familiarisé avec les concepts généraux de signature numérique, certificat, et infrastructure à clé publique, comme utilisé dans X.509, le DSG et le PAG.

Définitions

Ce document utilise les termes suivant :

Activation Data Les valeurs, autre que les clés, qui sont requis pour opérer des modules cryptographiques et qui nécessitent d'être protégés.

Authentification Le processus qui établis que les individus, organisation, ou autre sont qui ils prétendent être. Dans le contexte d'une PKI, l'authentification peut être le processus d'établissement qu'un individu ou organisation applique pour accéder à quelque chose sous un certain nom est, en fait, l'individu ou l'organisation propre. Cela correspond au deuxième processus impliqué dans l'identification.

CA-certificate Un certificat pour une clé publique de CA émise par une autre CA

Certificate Policy Un jeu nommé de règles qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou class d'applications avec des besoins de sécurités communs. Par exemple, un CP particulier peut indiquer l'applicabilité d'un type de certificat pour l'authentification des parties engagés dans des transaction b2b pour le commerce de biens ou de services dans une plage de prix donné.

Certification path Une séquence ordonnée de certificats qui, ensemble avec la clé publique de l'objet initial dans le chemin, peuvent être traités avec la clé publique de l'objet initial dans le chemin, peut être traité pour obtenir l'objet final est dans le chemin.

Certification Practice Statement Une déclaration des pratiques qu'une autorité de certification emploie en émettant, gérant, révoquant, et renouvelant les certificats.

CPS Summary (ou CPS Abstract) Un sous-jeu des dispositions d'une CPS complète qui est rendue publique par une CA.

Identification Les processus établissant l'identité d'un individu ou d'une organisation, par ex, pour montrer qu'un individu ou une organisation est un individu ou une organisation spécifique. Dans le contexte d'une PKI, l'identification réfère à 2 processus :

1. Établir qu'un nom donné d'un individu ou d'une organisation correspond à une identité du monde réel d'un individu ou d'une organisation
2. Établir qu'un individu ou une organisation s'applique pour un accès à quelque chose sous ce nom est, en fait, l'individu ou l'organisation nommée. Une identification d'une personne peut être un demandeur de certificat, un demandeur pour un emploie

dans un poste de confiance participant à une PKI, ou une personne cherchant accès au réseaux ou à une application, telle qu'un administrateur CA cherchant l'accès aux systèmes CA.

Issuing certification authority Dans le contexte d'un certificat particulier, la CA émettrice est la CA qui a émise le certificat.

Participant Un individu ou une organisation qui joue un rôle dans une PKI donnée comme un souscripteur, un tiers de confiance, CA, RA, etc.

PKI Disclosure Statement Un instrument qui complète une CP ou une CPS en divulguant des informations essentielles sur les stratégies et pratiques d'une CA/PKI. Un PDS est un véhicule pour divulguer et souligner les informations normalement couvertes en détail par les documents CP et/ou CPS associés. En conséquence, un PDS n'est pas prévu pour remplace une CP ou CPS.

Policy qualifier Information dépendante de la stratégie qui peut accompagner un identifiant de CP dans un certificat X.509. De telles informations peuvent inclure un pointeur vers une URL d'une CPS applicable ou d'un agrément de tiers de confiance. Il peut également inclure du texte qui contient les termes d'utilisation du certificat ou des informations légales.

Registration authority (RA) Une entité qui est responsable pour une ou plusieurs fonctions : l'identification et l'authentification des demandeurs de certificat, l'approbation ou le rejet des applications de certificat, initier les révocations de certificat ou leur suspension sous certaines circonstances, traiter les demandes de renouvellement ou changement de clé. Les RA, cependant, ne signent ou n'émettent pas de certificat.

Relying party Un destinataire d'un certificat qui agit en se fondant sur ce certificat et/ou toutes signature vérifiées en utilisant ce certificat. Dans ce document, les termes "certificate user" et "relying party" sont utilisé de la même manière.

Relying party agreement (RPA) Un agrément entre une autorité de certification et un tiers de confiance qui établis typiquement les droits et responsabilité entre ces parties en regardant la vérification des signatures ou d'autres utilisation des certificats.

Set of provisions Une collection de déclarations de stratégies et/ou de pratique, couvrant un éventails de sujets standards, à utiliser dans l'expression d'un CP ou CPS utilisant l'approche décrite dans ce framework.

Subject certification authority (subject CA) Dans le contexte d'un certificat CA particulier, le subjet CA est la CA dont la clé publique est certifiée dans le certificat

Subscriber Un Sujet d'un certificat qui a été émis.

Subscriber Agreement Un agrément entre une CA et un souscripteur qui établis les droits et responsabilités des parties en regardant l'émission et la gestion des certificats.

Validation Le processus d'identification des demandeurs de certificat. la validation est un sous-jeu de l'identification et réfère à l'identification dans le contexte d'établissement de l'identité des demandeurs de certificat.

Concepts

Cette section explique les concepts des CP et CPS, et décris leur relation avec d'autres documents PKI, tels que les agréments de souscripteur et de tiers de confiance. D'autres concepts liés sont également décris. Certains supports couverts dans cette section et dans d'autres sections sont spécifiques aux extensions de stratégie de certificat comme définis dans X.509v3. Excepté pour ces sections, ce framework est prévu pour être adaptable à d'autres formats de certificat qui peuvent être utilisés.

Certificate Policy

Quand une autorité de certification émet un certificat, elle fournis une déclaration à l'utilisateur du certificat qu'une clé publique particulière est liée à l'identité et/ou d'autres attributs d'une entité particulière. La mesure par laquelle le tiers de confiance devrait se conformer sur cette déclaration, cependant, doit être évalué par le tiers de confiance ou d'entité qui contrôle ou coordonne la manière dont les tiers de confiance ou les applications de confiance utilisent les certificats. Différents certificats sont émis suivant différentes pratiques et procédures, et peuvent être utilisable pour différentes applications et/ou buts.

Le standard X.509 définis une CP comme un jeu nommé de règles qui indique l'applicabilité d'un certificat à une communauté et/ou classe d'application particulier avec les pré-requis de sécurité communs. Un certificat X.509v3 peut identifier une CP applicable spécifique, qui peut être utilisé par un tiers de confiance pour décider de faire confiance ou non à un certificat, la clé publique associée ou les signatures numériques vérifiées en utilisant la clé publique pour un but particulier.

Il y a typiquement 2 catégories de CP. D'abord, certaines CP indiquent l'applicabilité d'un certificat à une communauté particulière. Ces CP présentent les pré-requis pour l'utilisation de certificat et les pré-requis des membres d'une communauté. Par exemple, une CP peut se

concentrer sur les besoins d'une communauté géographique, tel que les pré-requis de stratégie ETSI pour les CA émettant des certificats qualifiés. Également, une CP de ce type peut se focaliser sur les besoins d'une communauté de marché spécifique telle que les services financiers.

La seconde catégorie de CP indique l'applicabilité d'un certificat à une classe d'applications avec des pré-requis de sécurité communs. Ces CP identifient un jeu d'applications ou d'utilisations pour les certificats et indique que ces applications ou utilisations nécessitent un certain niveau de sécurité. Ils sont ainsi exposés aux exigences PKI qui sont appropriés pour cet applications ou utilisation. Une CP dans cette catégorie créé souvent des jeux de pré-requis appropriés pour un certain niveau d'assurance fournis par les certificats, relatifs aux certificats émis conformément aux CP liés. Ces niveaux d'assurance peuvent correspondre à des classes ou des types de certificat.

Par exemple, le Government of Canada PKI Policy Management Authority (GOC PMA) a établis 8 stratégies de certificat dans un seul document, 4 stratégies pour les certificats utilisé pour les signatures et 4 certificat pour les certificats utilisé pour le chiffrement. Pour chacune de ces applications, le document établis 4 niveaux d'assurances : rudimentaire, basique, moyen et élevé. Le GOC PMA décris certains types d'utilisation de signature numérique et de confidentialité, chacun avec un certain jeu de pré-requis de sécurité, et groupé en 8 catégories. Le GOC PMA établis ainsi les pré-requis PKI pour chacune de ces catégories, en créant 8 types de certificats, chacun fournissant des niveaux d'assurance rudimentaire, basique, moyen et élevé. La progression du niveau d'assurance rudimentaire à élevé correspond à l'augmentation du niveau de sécurité et d'assurance requis.

Une CP est représentée dans un certificat par un numéro unique appelé un OID. Cet OID, ou au moins un "arc", peut être enregistré. Un "arc" est le début d'une séquence numérique d'un OID et est assigné à une organisation particulière. Le processus d'enregistrement suit les procédures spécifiées dans les standards ISO/IETC et ITU. Le partie qui enregistre l'OID ou l'arc peut également publier le texte d'un CP, pour être examiné par les tiers de confiance. Tout certificat va explicitement déclarer une seule CP ou, possiblement, être émis en accord avec un petit nombre de stratégies différentes. De telles déclaration apparaissent dans l'extension de stratégie de certificat des certificats X.509v3. Quand une CA place plusieurs CP dans une extension de stratégie de certificat d'un certificat, la CA affirme que le certificat est approprié pour utilisation en accord avec une des CP listées.

Les CP constituent également une base pour un audit, accréditation, ou autre évaluation d'une CA. Chaque CA peut être évaluée avec une ou plusieurs stratégie de certificat ou CPS qui sont reconnus comme implémentés. Quand une CA émet un certificat CA pour une autre CA, le CA émettrice doit évaluer le jeu de stratégie de certificats pour lequel il trust le sujet. Le jeu évalué est ainsi indiqué par la CA émettrice dans le certificat CA. Le traitement logique du chemin de certification X.509 emploie ces indication CP dans son modèle de validation.

Exemples de stratégie de certification

Dans un but d'exemple, supposons que l'International Air Transport Association (IATA) s'engage à définir certaines stratégies de certificat pour l'utilisation dans l'industrie du transport aérien, dans une PKI opérée par IATA en combinaison avec les PKI opérés par les transports aériens individuels. 2 CP peuvent être définis - l'IATA General-Purpose CP, et l'IATA Commercial-Grade CP.

L'IATA General-Purpose CP pourrais être utilisé par l'industrie pour protéger les informations de routine (ex : mails) et pour authentifier les connexions depuis les navigateurs web vers les services d'informations générales. Les paires de clé sont générées, stockées, et gérées en utilisant des systèmes à base de logiciel et à faible coût, tels que les navigateurs commerciaux. Sous cette stratégie, un certificat peut être automatiquement émis à tous les employés dans l'annuaire de l'IATA ou un membre qui a envoyé une demande de certificat signée par le biais d'un administrateur réseaux dans son organisation.

L'IATA Commercial-Grade CP pourrait être utilisé pour protéger les transactions financières ou lier les échanges contractuels entre les entreprises. Sous cette stratégie, l'IATA pourrait imposer que les paires de clé certifiées soient générées et stockées dans des jetons hardwares cryptographiques approuvés. Les certificat et jetons pourraient être fournis aux employés avec une autorité de validation. Les individus autorisés peuvent ainsi être obligés d'être présents dans le bureaux de sécurité de l'organisation, montrer un badge d'identification valide, et signer un agrément de souscripteur qui leur impose de protéger le jeton et de l'utiliser seulement pour les buts autorisés.

Champs de certificat X.509

Les extensions X.509 suivant sont utilisés pour supporter les CP :

- Extension de stratégies de certificat
- Extension de mappage de stratégie
- Extension de contrainte de stratégie

Extension de stratégie de certificat

Un champ de stratégies de certificat liste les CP que l'autorité de certification déclare comme applicable. En utilisant l'exemple de l'IATA General-Purpose et Commercial-Grade définis plus haut, les certificats émis pour les employés normaux vont contenir l'identifiant d'objet pour la stratégie à but générale. Les certificats émis pour les employés avec autorité de validation vont contenir les identifiants d'objets pour les 2 stratégies. L'ajout des 2 stratégies dans les certificats signifie qu'ils sont appropriés pour les 2 stratégies. Ces stratégies de certificat peuvent également être optionnellement transmettre les valeurs de qualifiants pour chaque stratégie identifié.

En traitant un chemin de certification, un CP qui est acceptable pour l'application doit être présent dans tous les certificats dans le chemin, par ex., dans les certificats CA et les certificat EE.

Si le champ de stratégies de certificats est marqué critique, il sert le même but que décris plus haut mais a un rôle additionnel. Spécifiquement, il indique que l'utilisation du certificat est restreint à une des stratégies identifiées, par ex, l'autorité de certification déclare que le certificat doit seulement être utilisé en accord avec les dispositions d'au moins une CP listée. Ce champ est prévu pour protéger l'autorité de certification contre les réclamations pour des dommages causés par un tiers de confiance qui a utilisé le certificat dans un but inapproprié ou d'une manière inapproprié, comme stipulé dans la CP applicable.

Par exemple, l'Internal Revenue Service peut émettre des certificat pour les contribuables dans le but de protéger les déclarations fiscales. L'Internal Revenue Service peut comprendre et accommoder les risques lié à l'émission de mauvais certificat, par ex, à un imposteur. Supposons, cependant, que quelqu'un à utilisé un certificat comme base pour le chiffrement de secrets commerciaux à plusieurs millions de dollars, qui tombent ensuite dans de mauvaises mains suite à une attaque par cryptanalytique par un attaquant qui est capable de déchiffrer le message. L'Internal Revenue Service peut vouloir se défendre lui-même contre les réclamations de dégâts dans de telles circonstances en pointant la criticité de l'extension des stratégies de certificat pour montrer la mauvaise utilisation du certificat par le souscripteur et le tiers de confiance. L'extension de stratégies de certificat marquée critique est prévue pour limiter les risques de la CA dans de telles situations.

Extension de mappage de stratégie

L'extension de mappage de stratégie peut seulement être utilisé dans les certificats CA. Ce champ permet à une autorité de certification d'indiquer que certaines stratégies dans son propre domaine peuvent être considérés équivalents à d'autres stratégies dans le domaine du sujet de l'autorité de certification.

Par exemple, supposons que pour faciliter l'interopérabilité, l'ACE Corporation établis un agrément avec ABC Corporation pour cross-certifier les clés publiques de chaque autorité de certification pour sécuriser mutuellement leur échanges respectifs. De plus, supposons que les 2 entreprises ont des stratégies de protection de transaction financières pré-existantes appelées ace-e-commerce et abc-e-commerce, respectivement. On peut voir que générer simplement les cross-certificats entre les 2 domaines ne fournis pas l'interopérabilité, vu que les 2 applications d'entreprises sont configurées avec, en les certificats des employés sont renseignés avec, leur stratégies de certificat respectifs. Une possibilité est de reconfigurés toutes les applications financières pour imposer une des 2 stratégies et de ré-émettre tous les certificats avec les 2 stratégies apparaissant dans l'extension de stratégies de certificat. Une autre solution, qui peut être plus simple à administrer, utilise le champ de mappage de stratégie. Si ce champ est inclus dans un cross-certificat pour l'autorité de certification d'ABC Corporation émis par l'autorité de certification de ACE Corporation, il peut fournir une déclaration que la stratégie de protection des transactions financières de ABC (ex : abc-e-commerce) peut être considéré équivalent à celle de ACE Corporation (ex : ace-e-commerce). Avec une telle déclaration inclue dans le cross-certificat émis à ABC, les applications tiers dans le domaine ACE nécessitent la présence de l'identifiant d'objet pour que la CP ace-e-commerce soit également acceptée, traitée, et validée une fois les certificats émis dans le domaine ABC contenant l'identifiant d'objet pour la CP abc-e-commerce.

Extension de contraintes de stratégie

L'extension de contraintes de stratégie supporte 2 fonctionnalités optionnelles. La première est la capacité pour une autorité de certification de nécessiter que les indications de CP explicites soient présents dans tous les certificats suivant dans la chaîne de certification. Les certificats au début d'un chemin de certification peuvent être considérés par un tiers de confiance comme partie d'un domaine de confiance, par ex, les autorités de certification sont validés pour tous les buts donc aucune CP n'est nécessaire dans l'extension de stratégies de certificat. De tels certificats n'ont pas besoin d'indications explicites de CP. Quand une autorité de certification dans le domaine, cependant, certifie en dehors du domaine, il peut activer les pré-requis d'un CP qui doit apparaître dans les certificats suivants dans le chemin de certification.

L'autre fonctionnalité optionnelle dans le champ de contraintes de stratégie est la capacité pour une autorité de certification de désactiver le mappage de stratégie pour les autorités de certification suivant dans la chaîne de certification. Il peut être prudent de désactiver le mappage de stratégies en certifiant en dehors du domaine. Cela peut aider à contrôler les risques dus à des trusts de transitions.

Qualifiants de stratégie

Le champ d'extension de stratégies de certificat comporte une disposition pour le transport, avec chaque identifiant de CP, d'informations se stratégie dans le champ qualifier. Le standard X.509 ne mandate pas le but lequel ce champ est utilisé, ni ne décris la syntaxe pour ce champ. Les types de qualifiants de stratégie peuvent être enregistrés par une organisation.

Les types de qualifiants de stratégie suivant sont définis dans la rfc3280 :

a) Le CPS Pointer contient un pointer vers une CPS, sommaire de CPS, RPA, ou PDS publié par la CA. Le pointeur est sous la forme d'une URI.

b) Le User Notice contient une chaîne texte qui est affiché au souscripteur et les tiers de confiance avant l'utilisation du certificat. Le texte peut être un IA5String ou BMPString. Une CA peut invoquer une procédure qui nécessite que la prise de connaissance par le tiers de confiance des termes applicables et des conditions d'utilisation.

Les qualifiants de stratégie peuvent être utilisé pour supporter la définition de CP génériques ou paramétrisés. En fournissant la CP de base, les types de qualifiants de stratégie peuvent être définis pour transmettre, sur une base par-certificat, des détails de stratégie spécifiques additionnels qui complète la définition générique.

Déclaration de pratique de certification

Le terme certification practice statement (CPS) est définis par le DSG et PAG en tant que "déclaration de pratique qu'un autorité de certification emploie pour émettre des certificats". Comme statué plus haut, une CPS établis les pratiques concernant le cycle de vie des services en plus de l'émission, tel que la gestion de certificat (incluant la publication et l'archivage), la révocation, et le renouvellement. Dans le DSG, le ABA étend cette définition avec les commentaires suivants :

"Une déclaration de pratique de certification peut prendre la forme d'une déclaration par l'autorité de certification des détails de son système fiable et les pratiques qu'elle emploie dans ses opérations et dans le support d'émission d'un certificat." Cette forme de CPS est le type le plus commun, et peut varier en longueur et en niveau de détail.

Certaines PKI peuvent ne pas avoir besoin de créer de déclaration détaillée et approfondie des pratiques. Par exemple, la CA peut elle-même être le tiers de confiance et sera toujours conscient de la nature et de la fiabilité de ses services. Dans d'autres cas, une PKI peut fournir des certificats fournissant seulement un très bas niveau d'assurance où les applications à sécuriser peuvent causer seulement des risques marginaux s'il sont compromis. Dans ces cas, une organisation établissant une PKI peut seulement vouloir écrire ou avec des CA utilisant un agrément de souscripteur, agrément de tiers de confiance, en fonction du rôle des différents participants de PKI. Dans de telles PKI, cet agrément peut servir comme seule déclaration de pratique utilisé par une ou plusieurs CA dans cette PKI. En conséquence, cet agrément peut également être considéré une CPS et peut être intitulé ou sous-titré comme tel.

Également, vu qu'une CPS détaillée peut contenir des détails sensible de son système, une CA peut choisir de ne pas publier l'entièreté du CPS. Elle peut choisir de ne publier qu'une CPS sommaire (ou CPS abstrait). La CPS sommaire contient seulement les dispositions de la

CPS que la CA considère être pertinents pour les participants dans la PKI (tel que les responsabilités des tiers ou les étapes du cycle de vie du certificat). Une CPS sommaire, cependant, ne contient pas les disposition sensibles de la CPS complète qui peut fournir à un attaquant les informations utiles sur les opérations de la CA. Tout au long de ce document, l'utilisation de CPS inclus la CPS détaillée et la CPS sommaire.

Les CPS ne constituent pas automatiquement des contrats et ne lie pas automatiquement les participants de la PKI comme un contrat le ferai. Lorsqu'un document sert de double objectif d'agrément de souscripteur ou tiers de confiance et CPS, le document est prévu pour être un contrat et constitue un contrat liant dans la mesure où un agrément de souscripteur ou de tiers de confiance serait considéré comme tel. La plupart des CPS, cependant, ne sont pas à double usage. Ainsi, dans beaucoup de cas, les termes de la CPS ont un effet lié comme termes de contrat seulement si un document séparé créé une relation contractuelle entre les parties et que ce document incorpore une partie ou toute la CPS en référence. De plus, si une PKI particulière emploie une CPS sommaire, la CPS sommaire peut être incorporé dans un agrément de souscripteur ou de tiers de confiance applicable.

Dans le future, un tribunal ou une loi statutaire ou réglementaire applicable peut déclarer qu'un certificat lui-même est un document qui est capable de créer une relation contractuelle, pour étendre ses mécanismes conçus pour être incorporé par référence (tel que l'extension de stratégies de certificat et ses qualifiants) indique que les termes d'utilisation apparaissent dans certains documents. Pendant ce temps, cependant, certains agréments de souscripteurs et tiers de confiance peuvent incorporer une CPS par référence et ainsi prendre ses dispositions sur les parties de tels accords.

Relation entre CP et CPS

Les CP et CPS adressent le même jeu de sujets qui sont d'interêt pour un tiers de confiance en terme de degré à et le but pour lequel un certificat à clé publique devrait être trusté. Leur principales différences sont dans le focus de leurs disposition. Un jeu CP énonce les pré-requis et les standards imposés par la PKI en respect de divers sujets. En d'autres termes, le but du CP est d'établir ce que les participants doivent faire. Une CPS, en contraste, status comment une CA et d'autres participants dans un domaine donné implémentent les procédures et contrôles pour répondre aux pré-requis statués dans la CP. En d'autres termes, le but de la CPS est de déclarer comment les participants effectuent leur fonction et implémentent les contrôles.

Une autre différence relate le périmètre de couverture des 2 types de document. Vu qu'une CP est une déclaration des pré-requis, il est préférable pour communiquer un guide d'exploitation minimum qui doivent être rencontrés par les PKI intéropérantes. Donc, une CP s'applique généralement à plusieurs CA, plusieurs organisations, ou plusieurs domaines. En contraste, une CPS d'applique seulement à une simple CA ou une simple organisation.

Un CA avec une seule CPS peut supporter plusieurs CP (utilisés pour différentes applications et/ou différentes communautés tiers de confiance). Également, plusieurs CA, avec des CPS différentes, peuvent supporter la même CP.

Par exemple, le gouvernement fédéral peut définir une CP globale au gouvernement pour gérer les informations de ressources humaines confidentielles. La CP sera une déclaration générale des pré-requis pour les participants dans la PKI du gouvernement, et une indication des types d'applications pour lesquelles elle est prévue. Chaque département ou agence souhaitant opérer une autorité de certification dans cet PKI peut nécessiter l'écriture de sa propre CPS pour supporter cette CP en expliquant comment elle gère les pré-requis de la CP. Dans le même temps, un CPS de département ou agence peut supporter d'autres stratégies de certificat.

Une autre différence entre une CP et une CPS concerne le niveau de détail des dispositions. Bien que le niveau de détail peut varier dans les CPS, une CPS va généralement être plus détaillée qu'un CP. Une CPS fournis une description détaillée des procédures et contrôles en places pour se conformer aux requis de la CP, alors que la CP est plus générale.

Les principales différences entre CP et CPS peuvent être résumés comme suit :

a) Une PKI utilise une CP pour établir les requis qui statuent sur ce que les participants doivent faire. Une simple CA ou organisation peut utiliser une CPS pour divulguer comment elle se conforme aux requis d'une CP ou comment elle implémente ses pratiques et contrôles.

b) Une CP facilite l'interopérabilité entre cross-certification, certification unilatérale, ou d'autres moyens. De plus, elle est prévue pour couvrir plusieurs CA. En contraste, une CPS est une déclaration d'une seul CA ou organisation. Son but n'est pas de simplifier l'interopération.

c) Une CPS est généralement plus détaillée qu'une CP et spécifie comment la CA se conforme aux requis spécifiés dans une ou plusieurs CP sous lesquelles elle émet des certificats.

En plus de populer l'extension de stratégies de certification avec l'OID de la CP applicable, une autorité de certification peut inclure, dans les certificats quelle émet, une référence à ses CPS.

Relation entre CP, CPS et d'autres documents

CP et CPS jouent un rôle centrale en documentant les pré-requis et pratiques d'une PKI. Cependant, ce ne sont pas les seuls documents. Par exemple, les agréments de souscripteur et les agréments de tiers de confiance jouent un rôle critique en allouant les responsabilités des souscripteur et tiers de confiance liés à l'utilisation de certificats et des paires de clé. Ils établissent les termes et conditions sous lesquelles les certificats sont émis, gérés, et utilisés. Le terme agrément de souscripteur est définis par le PAG comme : "un agrément entre une CA et un souscripteur qui établis les droits et obligation des parties au regard de l'émission et la gestion des certificats". Le PAG définis un agrément de tiers de confiance comme : "un agrément entre une autorité de certification et un tiers de confiance qui établis typiquement les droits et obligations entre ces parties au regard de la vérification des signatures numériques ou d'autres utilisations de certificats".

Comme mentionné précédemment, un agrément de souscripteur, un agrément de tiers de confiance, ou un agrément qui combine les 2 peut également service de CPS. Dans d'autres PKI, cependant, un agrément de souscripteur ou de tiers de confiance peut incorporer certains ou tous les termes d'une CP ou CPS par référence. D'autre PKI encore peuvent distiller depuis une CP et/ou CPS les termes qui sont applicables au souscripteur et place de tels termes dans un agrément de souscripteur auto-contenu, sans incorporer de CP ou CPS par référence. Elles peuvent utiliser la même méthode pour distiller les termes de tiers de confiance depuis une CP et/out CPS et placer de tels termes dans un agrément de tiers de confiance. Créer de tels agrément auto-contenus a l'avantage de créer des documents qui sont plus faciles à lire par les consommateurs. Dans certains cas, les souscripteur et les tiers de confiance peuvent être considérés comme des consommateurs sous une loi applicable, qui sont sujets aux lois civiles des pays, incorporer une CP ou une CPS par référence peut ne pas être efficace pour lier les consommateurs aux termes dans une CP ou CPS incorporé.

Les CP et CPS peuvent être incorporés par référence dans d'autres documents, incluant :

- Agréments d'interopérabilité (incluant les agréments entre les CA pour la cross-certification, la certification unilatérale, ou d'autres formes d'interopération).
- Agréments de vendeur (sous lequels un vendeur de PKI accepte de se conformer aux normes énoncées dans une CP ou CPS).
- Un PDS

Un PDS a une fonction similaire à une CPS sommaire. C'est un document relativement court contenant seulement un sous-jeu de détails critiques sur une PKI ou CA. Il peut différer d'une CPS sommaire, cependant, dans son but qui est d'agir comme sommaire d'information sur la nature globale de la PKI, en contraste à une forme condensée d'une CPS.

De plus, son but est de distiller les informations sur la PKI, en opposé à la protection d'information sensible de sécurité contenu dans une CPS non-publiée, bien qu'un PDS pourrait servir également cette fonction.

Tout comme un rédacteur pourrait souhaiter référer à une CP ou CPS ou l'incorporer par référence dans un agrément ou PDS, une CP ou CPS peut référer à d'autres documents lors de l'établissement des requis ou en définissant les déclarations. Par exemple, une CP pour définir les requis pour le contenu de certificat en se référant à un document externe énonçant un profile de certificat standard. Référencer des documents externes permet à une CP ou CPS d'imposer des requis détaillés ou des déclarations détaillées sans avoir à ré-écrire les dispositions longue depuis d'autres documents dans la CP ou CPS. De plus, référencer un document dans une CP ou CPS est une autre manière utile de diviser les dispositions entre les informations publique et les informations confidentielles sensibles (en plus de ou comme alternative à une CPS sommaire). Par exemple, une PKI peut souhaiter publier une CP ou CPS, mais maintenir les paramètres de construction du site pour une CA comme information confidentielle. Dans ce cas, la CP ou CPS pourrait référencer un manuel externe ou un document contenant ces paramètres détaillés.

Les documents qu'une PKI peut souhaiter faire référence dans une CP ou CPS incluent :

- Une stratégie de sécurité
- Manuels de formation, opérationnel, installation, et utilisateurs (qui peuvent contenir des requis opérationnels)

- Plans de gestion de clés
- Guides de ressources humaine et manuels d'embauche (qui peuvent décrire certains aspects de pratiques de sécurité personnel)
- Stratégie d'email (qui peut discuter des responsabilités des souscripteurs et tiers de confiance, aussi bien que les implications de gestion de clé, si applicable)

Jeu de disposition

Un jeu de dispositions est une collection de pratiques et/ou déclarations de stratégies, couvrant un éventail de sujets à utiliser dans l'expression d'une CP ou CPS employant l'approche décrite dans ce framework.

Une CP peut être exprimée comme un seul jeu de dispositions

Une CPS peut être exprimée comme un seul jeu de dispositions avec chaque composant adressant les requis d'une ou plusieurs stratégie de certificat, ou, alternativement, comme une collection organisée de jeux de dispositions. Par exemple, une CPS pourrait être exprimées comme un combinaison des éléments suivants :

a) Une liste de stratégies de certificats supportés par la CPS ;

b) Pour chaque CP dans (a), un jeu de dispositions qui contiennent les déclarations répondant à cette CP en ajoutant les détails non stipulés dans la stratégie ou expressément laissée à la discrétion de la CA (dans ses CPS) ; de telles déclarations servent à statuer comment cette CPS particulière implémente les requis d'une CP particulière, ou

c) Un jeu de dispositions qui contiennent des déclarations de pratique de certification dans la CA, sans regarder la CP.

Les déclarations fournies dans (b) et (c) peuvent augmenter ou affiner les stipulations de la CP applicable, mais ne doit généralement pas être en conflit avec une des stipulations d'une telle CP. Dans certains cas, cependant, une autorité de stratégie peut permettre des exceptions aux pré-requis dans une CP, parce que certains contrôles de compensation de la CA sont décris dans sa CPS, qui permet à la CA de fournir des assurances qui sont équivalents aux assurances fournies par les CA qui sont complètement conformes avec la CP.

Ce framework dessine le contenu d'un jeu de dispositions, en terme de 9 composants principaux, comme suit :

1. Introduction
2. Publication et dépôt
3. Identification et Authentification
4. Pré-requis opérationnels du cycle de vie de certificat
5. Installation, gestion, et contrôles opérationnels
6. Contrôles de sécurité techniques
7. Profiles de certificat, CRL, et OCSP
8. Audit de conformité
9. Autres affaires et questions juridiques

Les PKI peuvent utiliser ce simple framework de 9 composant primaires pour écrire une CP ou CPS simple. De plus, une CA peut utiliser ce framework pour écrire des agréments de souscripteur et/ou de tiers de confiance. Si une CA utilise ce framework pour construire un agrément, il peut utiliser le paragraphe 1 comme introduction, peut exposer les responsabilités des parties dans le paragraphe 2-8, et peut utiliser le paragraphe 9 pour couvrir les problèmes légaux et commerciaux décris plus en détail plus bas. L'ordre des sujets dans ce simple framework et les questions juridiques et de business est le même que l'ordre des sujets dans un logiciel typique ou d'autres agréments technologiques. Cependant, une PKI peut établir un jeu de documents centraux (avec une CP, CPS, agrément de souscripteur et de tiers de confiance) ayant tous la même structure et ordre des sujets, facilitant ainsi les comparaisons et les mappages entre ces documents et entre les documents correspondant d'autres PKI.

Ce simple framework peut également être utile pour les agrément autre que les agréments de souscripteur et de tiers de confiance. Par exemple, une CA souhaitant externaliser certains services à une RA ou une autorité de fabrication de certificat (certificate manufacturing authority (CMA)) peuvent trouver utile d'utiliser ce framework comme checklist pour écrire un agrément d'autorité d'enregistrement ou d'externalisation. Similairement, 2 CA peuvent souhaiter utiliser ce framework pour définir une cross-certification, certification unilatérale, ou d'autre agréments d'interopérabilité.

Les composants primaires du framework peuvent rencontrer les besoins des rédacteurs de CP, CPS et agréments cours. Cependant, ce framework est extensible, et sa couverture de 9 composants est suffisamment flexible pour s'adapter aux besoins des rédacteurs de CP et CPS. Spécifiquement, les composants apparaissant ci-dessus peuvent comprendre plusieurs éléments. La section suivante fournis une description plus détaillée du contenu des composants et leur sous-composants. Les rédacteurs de CP et CPS sont autorisés à ajouter des niveaux additionnels de sous-composants sous les sous-composant pour correspondre à leurs besoins.

Contenu du jeu de dispositions

Cette section étends le contenu du framework de dispositions. Les sujets identifiés dans cette section sont, en conséquence, des sujets candidats pour être inclus dans une CP ou CPS détaillée.

bien que de nombreux sujets sont identifiés, il n'est pas nécessaire pour une CP ou une CPS d'inclure une déclaration concrète pour chaque sujet. À la place, une CP ou CPS particulière peut indiquer "aucune stipulation" pour un composant, sous-composant, ou élément sur lequel la CP ou CPS n'impose aucun requis ou ne divulgue rien. En ce sens, la liste des sujets peut être considéré comme une checklist de sujets pour aider à la rédaction d'une CP ou CPS.

Il est recommandé que chaque composant et sous-composant soit inclus dans une CP ou CPS, même s'il n'y a aucune stipulation ; cela indique au lecteur qu'une décision consciente a été faite d'inclure ou exclure une disposition concernant ce sujet. Ce style de rédaction protège contre les oublis par inadvertance d'un sujet, tout en facilitant la comparaison de différentes stratégies de certificat ou CPS.

Dans une CP, il est possible de laisser certains composants, sous-composants et/ou élément non-spécifiés, et pour stipuler que les informations requises seront indiquées dans un qualifiant de stratégie, ou le document vers lequel le qualifiant de stratégie pointe. Le jeu de dispositions devrait référencer ou définir les types de qualifiant de stratégie requis et devrait spécifier les valeurs par défaut applicables.

1. Introductions

Ce composant identifie et introduit le jeu de dispositions, et indique les types d'entité et applications pour lesquels le document écris.

1.1 Vue générale

Ce sous-composant fournis une introduction générale au document. Ce sous-composant peut également être utilisé pour fournir un synopsis de la PKI pour laquelle la CP ou CPS s'applique. Par exemple, il peut définir différents niveaux d'assurance fournis par les certificats dans une PKI particulière, une représentation diagrammatique de la PKI être utile ici.

1.2 Nom du document et identification

Ce sous-composant fournis des noms applicable ou d'autres identifiants incluant les identifiants d'objets ASN.1, pour le document. Un exemple d'un tel nom de document serait "US Federal Government Policy for Secure E-mail".

1.3 Participants de la PKI

Ce sous-composant décris l'identité ou les types d'entités qui ont un rôle de participant dans une PKI :

Autorités de certification, Par ex, les entités qui émettent des certificat. Une CA est la CA émettrice respectant le certificat CA qui lui a été donné. Les CA peuvent être organisés hiérarchiquement dans laquelle une CA d'organisation émet des certificats à des CA opérés par des organisations subordonnées, comme une branche, une division, ou un département dans une plus grande organisation.

autorités d'enregistrement, par ex, les entités qui établissent les procédures d'enrôlement pour les candidats de certificats finaux, l'identification et l'authentification pour les candidats de certificats, et l'initialisation des demandes de révocation pour les certificats, et les approuver le renouvellement ou le changement de clé des certificats. Les organisations subordonnées dans une grande organisation peuvent agir comme RA pour la CA servant toute l'organisation, mais les RA peuvent également être externe à la CA.

souscripteurs des exemples de souscripteurs qui reçoivent des certificats d'une CA incluent les employés d'une organisation avec sa propre CA, les clients de banque ou de courtage, organisations hébergeant des sites de e-commerce, etc.

Tiers de confiance. Des examples de tiers de confiance incluent les employés d'une organisation ayant sa propre CA qui reçoit des emails signés par d'autres employs, les clients d'un site e-commerce, les organisations participant à un échange business-to-business, etc.

Autres participants, tels que les autorités de fabrique de certificat, les fournisseurs de services de dépôt, et d'autres entités fournissant des service liés à la PKI.

1.4 Utilisation de certificat

Ce sous-composant contient :

- Une liste ou les types d'applications pour lesquels les certificats émis sont utilisable, tels que les mails éléctroniques, les transactions de vente, contrats, ou ordre de voyage, et/ou
- Une liste ou les types d'applications pour lesquels l'utilisation des certificats est interdite.

Dans le cas d'une CP ou CPS décrivant différents niveaux d'assurance ce sous-composant peut décrire les application ou les types d'applications qui sont appropriés ou inappropriés pour les différents niveaux d'assurance.

1.5 Administration de stratégie

Ce sous-composant inclus le nom et l'adresse de l'organisation qui est responsable pour la rédaction, l'enregistrement, la maintenance, et la mise à jours de cette CP ou CPS. Il inclus également le nom, l'adresse email, numéro de téléphone, et numéro de fax d'une personne à contacter. Au lieu de nommer un personne, le document peut nommer un titre ou un rôle, un email alias, et d'autres informations généralisées. Dans certains cas, l'organisation peut statuer qui sa personne de contact, seule ou avec d'autre, est disponible pour répondre aux questions sur ce document.

De plus, quand une autorité de stratégie formelle ou informelle est responsable pour déterminer si une CA devrait être autorisée à opérer dans ou intéropérer avec une PKI, il peut être souhaitable d'approuver la CPS d'une CA comme étant utilisable pour l'a CP de l'autorité de stratégie. Si c'est le cas, ce sous-composant peut inclure le nom ou titre, adresse email, numéro de téléphone, fax, et autres informations généralisées de l'entité en charge de prendre de telles décisions. Finalement, dans ce cas, le sous-composant peut également inclure les procédures par lesquels cette détermination est faite.

1.6 Définitions et acronymes

Ce sous-composant contient une liste de définitions pour les termes définis utilisés dans ce document, aussi bien qu'une liste d'acronymes dans le document leur signification.

2 Responsablités de publication et de dépôt

Ce composant contient les dispositions applicable avec :

- Une identification de l'entité ou les entités qui opèrent les dépôts dans la PKI, tels qu'une CA, CMA, ou fournisseur de service de dépôt indépendant
- La responsabilité d'un participant de PKI pour publier les informations de pratiques, certificat, et le statuts courant de tels certificats, qui peuvent inclurent les responsabilités de rendre la CP ou CPS disponible au publique en utilisant divers mécanismes en identifiant les composants, sous-composants, et élément de tels documents qui existent mais ne sont pas publiquement disponible, par exemple, les contrôles de sécurité, les procédures de dédouanement, ou information secrètes.
- Quand les informations doivent être publiés et la fréquence de publication, et
- le contrôle d'accès sur les objets publiés incluant les CP, CPS, certificats, statuts de certificats, et CRL.

3 Identifiation et authentification

Ce composant décris les procédures utilisées pour authentifier l'identité et/ou les autres attributs d'un utilisateur demandant un certificat à une CA ou une RA avant de recevoir le certificat. En plus, le composant énonce les procédures pour authentifier l'identité et les critères d'accèptation des demandes des entités cherchant à devenir un CA, RA, ou d'autres entités opérant dans ou intéropérant avec la PKI. Il décris également comment les parties demande un renouvellement de clé ou une révocation sont authentifiés. Ce composant adresse également les pratiques de nommage, incluant la reconnaissance des droits de marque dans certains noms.

3.1 Nommage

Ce sous-composant inclus les éléments suivants pour le nommage et l'identification des souscripteurs :

- Les types et noms assignés au sujet, tel que les DN X.500, noms rfc822, et noms X.400.
- Si les noms doivent avoir un sens ou non
- Si les souscripteurs peuvent être anonymes ou des pseudonymes, et s'ils le peuvent, quels noms leur sont assignés ou peuvent être utilisé par les souscripteurs anonymes.
- Les règles pour interpréter divers formes de nom, tels que le standard X.500 et rfc822.
- Si les nom doivent être uniques, et
- La reconnaissance, l'authentification, et le rôle des marques.

3.2 Validation initiale de l'identité

Ce sous-composant contient les éléments suivant 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 d'une clé privée associée à la clé privée en cours d'enregistrement, par exemple, une signature numérique dans le message de demande de certificat.
- Les requis d'identification et d'authentification pour l'entité organisationnelle du souscripteur ou du participant (CA, RA, souscripteur, ou autre participant), par exemple, en consultant la base d'un service qui identifie les organisations ou en inspectant les statuts de l'organisation.
- Les requis d'identification et d'authentification pour un souscripteur ou une personne agissant pour le compte d'une organisation ou d'un participant (CA, RA, dans le cas de certificats émis aux organisation ou périphériques contrôles par une organisation, souscripteur, ou autre participant), incluant :

- Le type de documentation et/ou le nombre de référence d'identification requis.
- Comment une CA ou RA authentifie l'identité de l'organisation ou individu basé sur la documentation ou les accréditifs fournies
- Si l'individu doit se présenter personnellement à la CA ou RA authentifiante.
- Comment un individu tel qu'une personne de l'organisation est authentifiée, tels que par référence à des documents d'autorisation signés ou un badge d'identification d'entreprise.

- La liste des informations de souscripteur qui n'est pas vérifiée durant l'enregistrement initial
- La validation de l'autorité implique de déterminer si une personne a des droits spécifiques ou des permissions incluant la permission d'agir pour le compte d'une organisation pour obtenir un certificat ; et
- Dans le cas des applications par une CA souhaitant opérer dans, ou interopérer avec, une PKI, ce sous-composant contient le critère par lequel un PKI, CA, ou autorité de stratégie détermine si la CA est prévue pour de telles opérations ou intéropérations. Une telle intéropération peut inclure la cross-certification, certification unilatérale, ou d'autres formes d'intéropérations.

3.3 Identification et authentification pour les demande de renouvellement de clé

Ce sous-composant adresse les éléments suivant pour les procédures d'identification et d'authentification pour le renouvellement de clé pour chaque type de sujet (CA, RA, souscripteur, ou autres participants).

- les requis d'identification et d'authentification pour les routines de renouvellement de clé, tel qu'une demande de renouvellement de clé qui contient la nouvelle clé et est signée en utilisant la clé actuellement valide, et
- Les requis d'identification et authentification pour le renouvellement de clé après la révocation de certificat. Un exemple est l'utilisation du même processus que pour la validation initiale

3.4 Identification et authentification pour les demandes de révocation

Ce sous-composant décris les procédures d'identification et d'authentification pour une demande de révocation pour chaque type de sujet (RA, CA, souscripteur, et autres participants).

4 Requis opérationnel du cycle de vie des certificats

Ce composant est utilisé pour spécifier les requis imposés en émettant des CA, sujets de CA, RA, souscripteurs, ou autres participants en respect avec le cycle de vie d'un certificat.

Dans chaque cous-composant, des considérations séparées peuvent être nécessaire à donner au sujet d'une CA, RA, souscripteurs, et autres participants

4.1 Demande de certificat

Ce sous-composant est utilisé pour adresser les requis suivant au regard de la demande de certificat :

- Qui peut émettre une demande de certificat, tel qu'un sujet de certificat ou la RA ; et

- Le processus l'enrôlement utilisé par les sujets pour émettre des demandes de certificat et les responsabilités en connexion avec ce processus. Un exemple de ce processus est quand le sujet génère la paire de clé et envoie une demande à la RA. La RA valide et signe le demande et l'envoi à la CA. Une CA ou RA peut avoir la responsabilité d'établir le processus d'enrôlement pour pouvoir recevoir la demande. De même, les demandeurs de certificat peuvent avoir la responsabilité de fournir des informations précises sur leurs demandes de certificat.

4.2 Traitement des demandes de certificat

Ce sous-composant est utilisé pour décrire la procédure pour traiter les demandes de certificat. Par exemple, La CA et RA émettrice peut effectuer des procédures d'identification et d'authentification pour valider la demande de certificat. En suivant ces étapes, la CA ou RA va soit approuver soit rejeter la demande, éventuellement basé sur certains critères. Finalement, ce sous-composant définis la durée limite qu'une CA et/ou RA doit agir et traiter la demande.

4.3 Émission de certificat

Ce sous-composant est utilisé pour décrire les éléments suivant lié à l'émission de certificat :

- Les actions effectuées par la CA durant l'émission du certificat, par exemple une procédure par laquelle la CA valide la signature de la RA et l'autorité RA et génère un certificat ; et
- Les mécanismes de notification, s'il y'en a, utilisé par la CA pour notifier le souscripteur de l'émission du certificat ; par exemple, la procédure par laquelle la CA envoie par e-mail le certificat au souscripteur ou la RA ou les informations permettant au souscripteur de télécharger le certificat depuis un site web.

4.4 Acceptation de certificat

Ce sous-composant adresse les éléments suivant :

- La conduite d'un candidat qui sera considéré pour constituer l'acceptation du certificat. Une telle conduite peut inclure des étapes d'affirmation pour indiquer l'acceptation, les actions impliquant l'acceptation, ou un rejet du certificat ou de son contenu. Par exemple, l'acceptation peut être considéré si la CA n'a pas reçu de notification du souscripteur dans une certaine période de temps ; un souscripteur peut envoyer un message signé acceptant le certificat ; ou un souscripteur peut envoyer un message signé rejetant le certificat qui inclus la raison du rejet et identifie les champs dans le certificat qui sont incorrect ou incomplets.
- La publication du certificat par la CA. Par exemple, la CA peut poster le certificat dans un annuaire LDAP ou X.500.
- La notification de l'émission du certificat par la CA à d'autres entités. Par exemple, la CA peut envoyer le certificat à la RA.

4.5 Utilisation du certificat et de la paire de clé

Ce sous-composant est utilisé pour décrire les responsabilités liées à l'utilisation des clés et des certificats, incluant :

- La responsabilité du souscripteur lié à l'utilisation de la clé privée et du certificat du souscripteur. Par exemple, on peut imposer au souscripteur d'utiliser un clé privée et un certificat uniquement pour les applications appropriées comme indiquée dans la CP et en consistance avec le contenu du certificat (ex : le champ keyUsage). L'utilisation d'une clé privée et d'un certificat sont sujet aux termes de l'agrément du souscripteur, l'utilisation de la clé privée est permise seulement après que le souscripteur a accepté le certificat correspondant, ou le souscripteur doit arrêter l'utilisation de la clé privée après l'expiration ou la révocation du certificat.
- Les responsabilités des tiers de confiance liés à l'utilisation d'une clé publique de souscripteur et du certificat. Par exemple, un tiers de confiance peut être obligé de valider les certificats seulement pour les applications appropriées comme indiqué dans la CP et en

consistance avec le contenu du certificat (ex : le champ keyUsage), exécuter avec succès les opération de clé publique comme condition de validation d'un certificat, assumer la responsabilité de vérifier le statut d'un certificat en utilisant un des mécanismes requis ou permis définis dans la CP/CPS, et le consentement des termes de l'agrément du tiers de confiance comme condition de validation de certificat.

4.6 Renouvellement de certificat

Ce sous-composant est utilisé pour décrire les éléments suivants liés au renouvellement de certificat. Le renouvellement de certificat signifie l'émission d'un nouveau certificat au souscripteur sans changer le souscripteur ou d'autres clé publiques du participant ou informations dans le certificat :

- Les circonstances sous lesquelles le renouvellement du certificat prend place, tel que lorsque le certificat a expiré, mais la stratégie permet de réutiliser la même paire de clé.
- Qui peut faire des demandes de renouvellement de certificat, par exemple, le souscripteur, la RA, ou la CA peut automatiquement renouveler un certificat EE.
- Les procédures de CA ou RA pour traiter les demandes de renouvellement pour émettre le nouveau certificat, par exemple, l'utilisation d'un jeton, tels qu'un mot de passe, pour ré-authentifier le souscripteur, ou les procédures qui sont les même qui l'émission d'un certificat initial.
- La notification d'un nouveau certificat au souscripteur
- La conduite constituant l'acceptation du certificat
- La publication du certificat par la CA
- La notification de l'émission du certificat par la CA à d'autres entités.

4.7 Renouvellement le clé

Ce sous-composant est utilisé pour décrire les éléments suivants liés à un souscripteur ou un autre participant générant une nouvelle paire de clé et application pour l'émission d'un nouveau certificat qui certifie la nouvelle clé publique :

- Les circonstances sous lesquelles le renouvellement de clé de certificat peut ou doit être fait, tels qu'après la révocation d'un certificat pour une raison de compromission de clé ou après qu'un certificat a expiré et que la période d'utilisation de la paire de clé a également expiré.
- Qui peut demander le renouvellement le clé de certificat, par exemple, le souscripteur
- Les procédures CA ou RA pour traiter les demandes de renouvellement de clé pour émettre le nouveau certificat, tel que les procédures qui sont les même que pour l'émission de certificat initial.
- La notification du nouveau certificat au souscripteur
- La conduite constituant l'acceptation du certificat
- La publication du certificat par la CA
- La notification de l'émission du certificat par la CA à d'autres entités.

4.8 Modification de certificat

Ce sous-composant est utilisé pour décrire les éléments suivant liés à l'émission d'un nouveau certificat du à des changement d'informations dans le certificat autre qui la clé publique :

- Les circonstances sous lesquelles la modification de certificat peut se faire, tels qu'un changement de nom, changement de rôle, réorganisation résultant en un changement dans le DN.

- Qui peut effectuer des demandes de modification de certificat, par exemple, les souscripteurs, personnel des ressources humaines, ou la RA.
- Les procédures CA ou RA pour traiter les demandes de modification pour émettre le nouveau certificat, tel que les procédures qui sont les même que pour l'émission initiale.
- Notification du nouveau certificat au souscripteur
- La conduite constituant l'acceptation du certificat
- La publication du certificat par la CA
- La notification de l'émission du certificat par la CA à d'autres entités.

4.9 Révocation et suspension de certificat

Ce sous-composant adresse les points suivants :

- Les circonstances sous lesquelles un certificat peut être suspendu et les circonstances sous lesquelles il doit être révoqué, par exemple, dans le cas ou un souscripteur termine sont contrat, perd son jeton cryptographique, ou suspecte la compromission de la clé privé
- Qui peut demander la révocation du certificat du participant, par exemple, le souscripteur, RA ou CA dans le cas d'un certificat EE.
- Les procédures utilisées pour les demandes de révocation de certificat, tels qu'un message signé numériquement de la RA, du souscripteur, ou un appel téléphonique de la RA.
- La période de grâce disponible au souscripteur, dans laquelle le souscripteur doit créer une demande de révocation.
- Le temps dans lequel la CA doit traiter la demande de révocation
- Les mécanismes, s'il y en a, que le tiers de confiance peuvent utiliser ou doivent utiliser pour vérifier le statut des certificats qui souhaitent valider.
- Si un mécanisme de CRL est utilisé, la fréquence d'émission
- Si un mécanisme de CRL est utilisé, le délai maximum entre la génération de la CRL et sa publication (en d'autres termes, le temps maximum de traitement)
- La disponibilité d'un mécanisme de vérification on-line, par exemple, OCSP.
- Les pre-requis des tiers de confiance pour effectuer des vérification de statut/révocation on-line
- D'autres formes d'annonce de révocation disponible
- Toutes variations des stipulations précédentes pour lesquelles la suspension ou la révocation est le résultat d'une compromission de clé privée
- Les circonstances sous 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 utilisateur.
- Les procédures pour demander la suspension du certificat, tel qu'un message signé numériquement du souscripteur ou d'un RA, un appel téléphonique de la RA
- La durée de suspension

4.10 Services de statut de certificat

Ce sous-composant adresse les services de vérification de statut de certificat disponible aux tiers de confiance, incluant :

- Les caractéristiques opérationnelles des services de vérification de statut de certificat
- La disponibilité de tels services, et toutes stratégies applicables sur l'indisponibilité
- Toutes fonctionnalités optionnelles de tels services.

4.11 Fin de souscription

Ce sous-composant adresse les procédures utilisée pour les souscripteurs pour terminer la souscription des services CA, incluant :

- La révocation des certificat à la fin de la souscription (qui peut différer, en fonction de si la fin de souscription est dûe à l'expiration du certificat ou la fin du service).

4.12 dépôt et récupération de clé

Ce sous-composant contient les éléments pour identifier les stratégies et pratiques liées au dépôt, et/ou récupération des clés privées quand des services de dépôt de clés privée sont disponibles.

- Identification du document contenant les stratégies et pratiques de dépôt de clé et de récupération ou une liste de telles stratégies et pratiques
- Identification du document contenant les stratégies et pratiques d'encapsulation des clés de session ou une liste de telles stratégie et pratiques.

5. Gestion, opérationnel, et contrôles physiques

Ce composant décris les contrôles de sécurité non-techniques (c'est à dire, les contrôles physiques, procédurales et personnelles) utilisées par la CA émettrice pour effectuer de manière sécurisée les fonctions de génération de clé, authentification du sujet, assurances de certificat, révocation de certificat, audit, et archivage.

Ce composant peut également être utilisé pour définir des contrôles de sécurité non-techniques sur les dépôt, tels que les sujets CA, RA, souscripteurs, et autres participants. Les contrôles de sécurité non-techniques pour les CA, RA, souscripteurs, et autres participants peuvent être les mêmes, similaires, ou très différents.

Ces contrôles de sécurité non-techniques sont critique pour valider les certificat vu qu'un manque de sécurité peut compromettre les opérations CA résultantes par exemple, en la création de certificats ou CRL avec des informations erronées ou la compromission de la clé privée de la CA.

Dans chaque sous-composant, des considérations séparées vont, en général, être donnés à chaque type d'entité.

5.1 Contrôles de sécurité physiques

Dans ce sous-composant, les contrôles physiques sur les installation abritant les systèmes de l'entité sont décris :

- La construction et l'emplacement du site, tel que la pré-requis de construction pour des zones à haute sécurité et l'utilisation de salles fermées, cages, coffre-fort, et armoires.
- L'accès physique, par ex, les mécanismes de contrôles d'accès d'une zone à une autre ou l'accès à des zones de haute sécurité, tels que les opérations CA localisées dans une salle information sécurisée et supervisée par des gardiens ou des alarmes de sécurité.
- Puissance et climatisation
- Exposition à l'eau
- Prévention et protection contre le feu
- Stockage, par exemple, la nécessité d'un stockage de sauvegarde dans un emplacement séparé qui est sécurisé physiquement et protégé du feu et de l'eau.

- L'élimination des déchets
- sauvegarde hors-site

5.2 Contrôles procédurales

Dans ce sous-composant, les pré-requis opur reconnaître les rôles de confiance sont décris, avec les responsabilités de chaque rôle. Des exemples de rôles de confiance incluent les administrateurs systèmes, les responsables de la sécurité, et les auditeurs système.

Pour chaque tâche identifié, le nombre d'individus requis pour effectuer la tâche devrait être statué pour chaque rôle. L'identification et l'authentification requis pour chaque rôle peut également être définis.

Ce composant inclus également la séparation des privilèges en termes de rôles qui ne peuvent pas être effectués par les même individus.

5.3 Contrôles de sécurité personnel

Ce sous-composant adresse les éléments suivant :

- Qualifications, expérience, et habilitations que le personnel doit avoir comme condition pour jouer ces rôles de confiance ou d'autres rôles importants. Par exemple les accréditifs, expérience professionnelle, et habilitations gouvernementales que les candidats à ces positions doivent avoir.
- La vérification des antécédents et des procédures d'habilitations qui sont requis dans le cadre de l'embauche de personnel remplissant des rôles de confiance ou d'autres rôles importants ; de tels rôles peuvent nécessiter une vérification de leur casier judiciaire, références, et habilitations additionnelles qu'un participant engage après une décision d'embauche d'une personne particulière.
- Formations requises et procédures de formations pour chaque rôle qui suivent l'embauche.
- Toute période de renouvellement et les procédures de renouvellement pour chaque rôle après l'achèvement de la formation initiale.
- La fréquence et la séquence de la rotation des postes sur divers rôles
- Les sanctions contre le personnel pour les actions non autorisées, l'utilisation d'autorité non autorisée, l'utilisation non autorisé des systèmes dans le but d'imposer la responsabilité sur un participant.
- Les contrôles du personnel qui sont des indépendant aux lieu d'employés de l'entité, par exemple :
  - Exigences de cautionnement sur le personnel sous contrat
  - Les exigences contractuelles, y compris l'indemnisation des dommages dûs à des actions du personnel en contrat
  - L'audit et la supervision du personnel en contrat
  - D'autres contrôles sur le personnel en contrat
- La documentation à fournir au personnel durant la formation initiale, le renouvellement, ou autre.

5.4 Procédures d'audit de connexion

Ce sous-composant est utilisé pour décrire les évènements de connexion et les systèmes d'audit, implémentés dans le but de maintenir un environnement sécurisé.

- Les types d'évènements enregistrés, tels que les opérations sur le cycle de vie des certificats, tentatives d'accès au système, et requêtes faites au système.
- Fréquence à laquelle les logs d'audits sont traités ou archivés, par exemple, chaque semaine, suivant un évènement anormal ou d'alerte, ou quand le log d'audit est plein.
- Période pour laquelle les données d'audit sont conservées

- Protection des logs d'audit :
  - Qui peut voir les logs d'audit, par exemple, les administrateurs d'audit
  - La protection contre la modification des logs d'audit, par exemple une exigence qu'aucune modification ou suppression les enregistrements d'audit ou que seul l'administrateur d'audit peut supprimer un fichier d'audit comme partie de la rotation du fichier d'audit
  - Protection contre la suppression des logs d'audit.
- Procédures de sauvegarde des log d'audits
- Si le système de d'accumulation des logs d'audits est interne ou externe à l'entité
- Si le sujet qui à causé un évènement d'audit est notifié de l'action d'audit
- L'évaluation des vulnérabilité, par exemple, où les données d'audit sont lancées via un outils qui identifie les tentatives potentielles pour casser le système de sécurité

5.5 Archivage des données d'enregistrement

Ce sous-composant est utilisé pour décrire les stratégies d'archivage des enregistrements :

- Les types d'enregistrement qui sont archivés, par exemple, toutes les données d'audit, les information d'application de certificat, et la documentation supportant les applications de certificat.
- La période de rétention pour une archive
- La protection d'une archive
  - Qui peut voir l'archive, par exemple, seulement l'administrateur d'audit
  - La protection contre la suppression de l'archive
  - La protection contre la détérioration du support sur lequel l'archive est stockée, tel que la migration des donnée périodiquement sur un nouveau support.
  - La protection contre l'obsolescence du matériel, systèmes d'exploitation et autres logiciels.
- Les procédure de sauvegarde des archives
- Les pré-requis pour l'horodatage des enregistrements
- Si le système de collecte d'archive est interne ou externe
- Les procédures pour obtenir et vérifier les informations d'archive, tels que le besoin de maintenir 2 copies de l'archive sous le contrôle de 2 personnes, et que les 2 copies soient comparées pour s'assurer que les informations sont valides.

5.6 Renouvellement des clés

Ce sous-composant décris les procédures pour fournir une nouvelle clé aux utilisateurs de la CA après un renouvellement de clé par la CA. Ces procédures peuvent être les même que les procédures pour fournir la clé courante. Également, la nouvelle clé peut être certifiée dans un certificat signé en utilisant l'ancienne clé.

5.7 Récupération après sinistre ou compromission

Ce sous-composant décris les pré-requis liées à la notification et les procédures de récupérations dans le cas d'une compromission ou d'un sinistre. Chaque point suivant doit être adressé séparément

- L'identification ou la liste des incidents et compromissions applicable et les procédure de gestion et de reporting.
- Les procédures de récupération utilisée si les ressources informatiques, logiciels et/ou données sont corrompues ou suspectée comme tel. Ces procédures décrivent comment un environnement sécurisé est ré-établis, quels certificats sont révoqués, si la clé de l'entité est révoquée, comme la nouvelle clé publique 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 est ré-établis, comme la nouvelle clé de l'entité publique est fournie aux utilisateurs, et comment les sujets sont re-certifiés.
- Les capacités de l'entité pour s'assurer de la continuité du business après un sinistre naturel ou autre. De telles capacités peuvent inclure la disponibilité d'un site distant sur lequel les opérations peuvent être récupérées. Il peut également inclure les procédures pour sécuriser ses facilités durant la période de temps suivant un désastre naturel ou autre et avant un rétablissement d'un environnement sécurisé, soit sur le site original, soit sur un site distant. Par exemple, les procédures pour protéger contre le vol de matériel sensible sur un site endommagé par un séisme.

5.8 Cessation de CA ou RA

Ce sous-composant décris les requis liées aux procédures pour la notification de cessation et la cessation d'une CA ou RA, incluant l'identité du gardien des documents d'archive de la CA ou RA.

6. Contrôles de sécurité technique

Ce composant est utilisé pour définir les mesures techniques prises par la CA émettrice pour protéger ses clés cryptographique et données d'activation (par ex, PIN, mot de passe, ou clé partagées gérées manuellement). Ce composant peut également être utilisé pour imposer des contraintes sur les dépôts, sujets CA, souscripteur, et autres participants pour protéger leur clés privées, données d'activation pour leur clé privées, et paramètres de sécurité critique. La gestion de clé sécurisé est critique pour s'assurer que tous les secrets et clés privées et données d'activation sont protégées et utilisés seulement par le personnel autorisé.

Ce composant décris également d'autres contrôles de sécurité technique utilisées par la CA émettrice pour effectuer les fonctions sécurisées de génération de clé, d'authentification de l'utilisateur, d'enregistrement de certificat, de révocation de certificat, d'audit, et d'archivage. Les contrôle techniques incluent les contrôle de sécurité du cycle de vie (incluant la sécurité de l'environnement de développement logiciel, la méthodologie de développement logiciel) et les contrôles de sécurité opérationnel.

Ce composant peut également être utilisé pour définir d'autres contrôles de sécurité technique sur les dépôts, sujets CA, RA, souscripteurs, et autres participants.

6.1 Génération et installation de paire de clé

La génération et l'installation de paire de clé doit être considéré pour la CA émettrice, les dépôts, sujets de CA, RA, et souscripteurs. Pour chacun de ces types d'entité, les questions suivantes peuvent potentiellement être répondues :

1. Qui génère l'entité publique, la paire de clé ? Cela peut être le souscripteur, la RA, ou la CA. Également, comment est effectuée la génération de la clé ? Est-ce que la génération de clé est faite par un hardware ou un software ?
2. Comment est fournie la clé privée à l'entité de manière sécurisée ? Par exemple, une situation où l'entité l'a généré et donc l'a déjà, qui manipule physiquement la clé privée, envoie un jeton contenant la clé privée de manière sécurisée ou en la délivrant dans une session SSL.
3. Comment la clé publique de l'entité est fournie de manière sécurisée à l'autorité de certification ? Certaines possibilités sont dans une session SSL ou dans un message signé par la RA.
4. Dans le cas de la CA, comment la clé publique de la CA est fournie aux tiers de confiance de manière sécurisée.
5. Quels sont les tailles de clé ?
6. Qui génère les paramètres de la clé publique, et est-ce que la qualité des paramètres sont vérifiés durant la génération ?
7. Dans quel but la clé peut être utilisée, ou quel usage de clé est interdite ? Pour les certificats X.509v3, ces but devraient être mappés dans les flags d'utilisation de clé.

6.2 Contrôles de Protection de clé privé et de module cryptographique

Les pré-requis pour la protection de la clé privée et des modules cryptographiques doivent être considérés pour la CA emettrice, les dépôts, les sujets de CA, RA, et souscripteurs. Pour chacun de ces types ou entités, les questions suivantes doivent être répondue :

1. Quels standards, s'il y en a, sont requis pour le module cryptographique utilisé pour générer les clé ? Un module cryptographique peut être composé de hardware, software, firmware, ou une combinaison. Par exemple, est-ce que les clé certifiées par l'infrastructure doivent être générés en utilisant des modules conformes FIPS 140-1 ? Si c'est le cas, quel est le niveau FIPS 140-1 du module ? Y'a t'il une autre ingénierie ou d'autres contrôles liés au module cryptographique, tel que l'identification des limites du module cryptographique, l'entrée/sortie, les rôles et services, l'état de la machine, la sécurité physique, la sécurité logiciel, la sécurité du système d'exploitation, la conformité des algorithmes, la compatibilité éléctro-magnétique, et les selfs tests.
2. Est-ce que la clé privée est sous contrôle de n de m personnes. Si c'est le cas, fournir n et m (2 contrôleurs est un cas spécial où n=m=2)
3. Est-ce que la clé privée est entiercée ? si c'est le cas, qui est l'agent d'entièrcement, sous quelle forme est la clé entiercée (texte clair, chiffré, splitté), et quels sont les contrôles de sécurités dans le système d'entièrcement ?
4. Est-ce que la clé privée est sauvegardée ? Si c'est le cas, qui est l'agent de sauvegarde, sous quelle forme est la clé sauvegardée, et quels sont les contrôles de sécurité dans le système de sauvegarde ?
5. Est-ce que la clé privée est archivée ? Si c'est le cas, qui est l'agent d'archivage, sous quelle forme est archivée la clé, et quels sont les contrôles de sécurité dans le système d'archivage ?
6. Sous quelles circonstances, s'il y en a, la clé privée peut être transférée dans ou depuis un module cryptographique ? Qui est autorisé à effectuer une telle opération de transfert ? Sous quelle forme est la clé privée durant le transfert ?
7. Comment est stocké la clé privée dans le module ?
8. Qui peut activer (utiliser) la clé privée ? Quelles actions doivent être effectués pour activer la clé privée (ex : login, mise en route, fournir un PIN, insérer la clé/jeton, automatique, etc.) ? Une fois la clé activée, est-ce que la clé est active pour une période indéfinie, active pour une seule fois, ou pour une période définie ?
9. Qui peut désactiver la clé privée et comment ? des exemples des méthodes de désactivation de clés privée incluent la déconnexion, suppression de la clé/jeton, désactivation automatique, et date d'expiration.
10. Qui peut détruire la clé privée et comment ? Par exemple, la remise symbolique, la destruction symbolique, et écraser la clé.
11. Fournir les capacité du module cryptographique dans les zones suivantes : identification des limites du module cryptographique, entrée/sortie, rôles et services, état de la machine, sécurité physique, sécurité logiciel, sécurité du système d'exploitation, conformité des algorithmes, compatibilité éléctromagnétique, et selfs tests. Les capacités peuvent être exprimés via une référence de conformité avec un standard tel que FIPS 140-1 et le niveau associé.

6.3 Autres aspects de la gestion de paire de clés

D'autres aspects de gestion de clé doivent être considérés pour la CA émettrice, les dépôts, les sujets CA, RA, souscripteurs, et d'autres participants. Pour chacun de ces types d'entité, les questions suivante ont potentiellement besoins d'être répondues :

1. Est-ce que la clé publique est archivée ? Si c'est le cas, qui est l'agent d'archivage et quels sont les contrôles de sécurité sur le système d'archivage ? Également, quel logiciel et hardware doit être conservé comme partie de l'archive pour permettre d'utiliser la clé publique dans le temps ? Note : ce sous-composant n'est pas limité aux requis aux pré-requis ou à la description de l'utilisation des signatures numériques avec les données d'archive, mais peut adresser les contrôles d'intégrité autre que les signatures numériques quand une archive nécessite une protection contre l'altération. Les signatures numériques ne fournissent pas de protection contre l'altération ou de protection de l'intégrité des données ; Elles vérifient simplement l'intégrité des données. De plus, la période d'archivage peut être supérieur à une signature numérique appliquée à la donnée archivée.
2. Quel est la période opérationnelle des certificats émis au souscripteur. Quelles périodes d'utilisation, ou durée de vie, pour les paires de clé du souscripteur ?

6.4 Données d'activation

Les données d'activation réfèrent aux valeurs de données autre que les clé privées qui sont nécessaire pour opérer les clés privées ou les modules cryptographique contenant les clés privées, tels qu'un PIN, passphrases, ou portions d'une clé privée utilisées dans un schéma de splitting de clé. La protection des données d'activation empêchent l'utilisation non autorisée de la clé privée, et les besoins potentiels à considérer pour la CA émettrice, les sujets CA, RA, et les souscripteurs. Une telle considération nécessite potentiellement d'adresser tout le cycle de vie des données d'activation depuis la génération jusqu'à l'archivage et la destruction. Pour chaque types d'entité (CA émettrice, sujets CA, RA, souscripteur, et autres participants), toutes les questions listées en 6.1 à 6.3 peuvent potentiellement être répondus en respect des données d'activation au lieu du respect des clés.

6.5 Contrôles de sécurité informatique

Ce sous-composant est utilisé pour décrire les contrôles de sécurité informatique tels que : l'utilisation de concept de base de calcul de confiance, le contrôle d'accès discrétionnaire, le contrôle d'accès obligatoire, la réutilisation d'object, l'audit, d'identification et l'authentification, les chemin de confiance, les tests de sécurité, et les tests de pénétration. L'assurance de produit peut également être adressé.

Un taux de sécurité informatique pour les systèmes informatiques peut être requis. Le taux peut être basé, par exemple, sur le Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), ou le Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408 :1999. Ce sous-composant peut également adresser les requis pour l'analyse de l'évaluation de produit, tests, profilage, certification de produit, et/ou accréditation de produit lié à l'activité entreprise.

6.6 Contrôles de sécurité du cycle de vie

Ce sous-composant adresse les contrôles de développement système et les contrôles de gestion de la sécurité.

Les contrôles de développement système incluent la sécurité de l'environnement de développement, la sécurité du personnel de développement, la sécurité de la gestion de configuration durant la maintenance produit, les pratique d'ingénierie logiciel, la méthodologie de développement logiciel, la modularité, couches, l'utilisation de concepts à sécurité intégrée et implémentation technique et sécurité des facilités de développement.

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

Ce sous-composant peut également adresser le cycle de vie de la sécurité basé par exempel, sur Trusted Software Development Methodology (TSDM) niveau IV et V, independent life-cycle security controls audit, et Software Engineering Institute's Capability Maturity Model (SEI-CMM).

6.7 Contrôles de sécurité réseaux

Ce sous-composant adresse les contrôles liés à la sécurité des réseaux, incluant les firewalls.

6.8 Horodatage

Ce sous-composant adresse les requis ou pratiques liées à l'utilisation d'horodatage de diverses données. Il peut également discuter de si

l'application de l'horodatage doit utiliser une source de temps fiable.

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 utilisés, le format de CRL et/ou OCSP. Cela inclus les informations dans les profils, versions, et extensions utilisées.

7.1 Profil de certificat

Ce sous-composant adresse les sujets suivant, potentiellement par référence à une définition de profil séparé, tel que celui définis dans la rfc 3280.

- Les versions supportées
- Les extensions de certificat utilisées et leur criticité
- Les identifiant d'objet d'algorithmes cryptographiques
- Les formes de nom utilisé pour la CA, RA, et les noms des souscripteurs
- Les contraintes de nom utilisés et les formes de nom utilisé dans les contraintes de nom
- Les OID de CP applicable
- L'utilisation de l'extension de contrainte de stratégie
- La syntaxe et sémantiques des qualifiants de stratégie
- Les sémantiques de traitement pour l'extension critique CP

7.2 Profile de CRL

Ce sous-composant adresse les sujets suivant, potentiellement par référence à une définition de profil séparé, tel que celui définis dans la rfc 3280.

- Les numéro de version supportés
- Les extensions d'entrée de CRL utilisées et leur criticité

7.3 Profile OCSP

Ce sous-composant adresse les sujets suivant, potentiellement par référence à une définition de profil séparé, tel que celui définis dans la rfc 2560.

- La version d'OCSP qui est utilisé comme base pour établir un système OCSP
- Les extensions OCSP utilisés et leur criticité

8 Audit et autres évaluations de conformité

Ce composant adresse les sujets suivants :

- La liste des sujets couverts par l'évaluation et/ou la méthodologie d'évaluation utilisée pour effectuer l'évaluation ; par exemple WebTrust pour les CA et SAS 70.
- La fréquence de l'audit de conformité ou autres évaluations pour chaque entité qui doit être évalué conformément à une CP ou CPS, ou les circonstances qui vont déclencher une évaluation ; par exemple un audit annuel, évaluation pré-opérationnelle comme condition d'autorisation pour une entité d'être opérationnelle, ou des investigations suivant une possible compromission de la sécurité.
- L'identité et/ou les qualifications du personnel effectuant l'audit ou autre évaluation.
- La relation entre l'évaluateur et l'entité qui est évaluée, incluant le degré d'indépendance de l'évaluateur.
- Les actions prises en résultat de déficience trouvé durant l'évaluation ; par exemple, une suspension temporaire des opérations jusqu'à ce que la déficience soit corrigée, la révocation de certificats émis par l'entité évaluée, le changement de personnel, les investigations spéciales ou des évaluation de conformité plus fréquentes, et les demandes pour les dommages contre l'entité évaluée.
- Qui est habilité à voir les résultat d'une évaluation (ex, les entités évaluées, d'autres participant, tout le monde), qui leur fournis, et comment ils sont communiqués.

9 Autre questions juridiques et sur l'entreprise

Ce sous-composant couvre les questions juridiques et liées à l'entreprise. Les sections 9.1 et 9.2 discutent des questions d'entreprise de redevances à percevoir pour divers services et les responsabilités financières des participants pour maintenir les ressources pour les opérations en cours et pour le payements des jugements ou règlement en réponse aux allégations formulées contre eux. Les sections restantes sont plus généralement concernés par les sujets légaux.

À partir de la section 9.3, l'ordre des sujets est le même que l'ordre des sujets dans un agrément de licence logiciel ou autre agrément technologique. En conséquence, ce framework n'est pas seulement pour les CP et CPS, mais également associé aux agréments liés à la PKI, spécialement les agréments de souscripteur et de tiers de confiance. Cet ordre est prévu pour aider les avocats examinant les CP, CPS et autres documents qui adhèrent à ce cadre.

En respect à de nombreux sous-composant légaux dans ce composant, une rédacteur de CP ou CPS peut choisir d'inclure dans le document les termes et conditions qui s'appliquent directement aux souscripteurs ou tiers de confiance. Par exemple, une CP ou CPS peut énoncer les limitations de responsabilité applicables aux souscripteurs et tiers de confiance. L'inclusion des termes et conditions est plus approprié dans les cas où la CP ou CPS est elle-même un contrat ou partie d'un contrat.

Dans d'autres cas, cependant, la CP ou CPS n'est pas un contrat ou partie d'un contrat ; à la place, elle est configurée pour que ses termes et conditions soient appliquées aux parties par des documents séparés, qui peuvent inclure des agréments associés, tels qu'un agrément de souscripteur ou tiers de confiance. Dans ce cas, un rédacteur de CP peut écrire une CP de façon à exiger que certaines conditions juridiques apparaissent (ou n'apparaissent pas) dans de tels agréments. Par exemple, une CP pour inclure un sous-composant statuant qu'un certain terme de limitation de responsabilité apparaisse dans les agréments de souscripteur et de tiers de confiance. Un autre exemple est une CP qui contient un sous-composant interdisant l'utilisation d'un agrément de souscripteur ou de tiers de confiance contenant une limitation de la responsabilité de la CA incompatible avec les disposition de la CP. Un rédacteur de CPS peut utiliser des sous-composants légaux pour divulguer que certains termes et conditions apparaissent dans des agréments de souscripteur, de tiers de confiance, ou d'autres, associé, utilisé par la CA. Une CPS peut expliquer, par exemple, que la CA écris qu'elle utilise un agrément de souscripteur ou de tiers de confiance associé qui applique une disposition particulière pour limiter la responsabilité.

9.1 Honoraires

Ce sous-composant contient les dispositions applicables liés aux frais des CA, dépôts, ou RA, tels que :

- frais d'émission ou de renouvellement de certificat
- frais d'accès au certificat
- frais d'accès aux informations de status ou de révocation
- frais pour d'autres services tels que ceux fournissant l'accès aux CP ou CPS

- Stratégies de remboursement

9.2 Responsabilité financière

Ce sous-composant contient les pré-requis ou les informations relatives aux ressources disponible aux CA, RA, et autres participants fournissant des services de certification pour supporter l'exécution de leurs responsabilité opérationnels, et pour rester solvable et payer les dommages dans le cas où ils sont tenus de payer un jugement ou un règlement dans le cadre d'une réclamation résultant de ces opérations. De telles dispositions incluent :

- Une déclaration que le participant maintient un certain montant de couverture d'assurance pour ses engagements envers les autres participants.
- Une déclaration que le participant a accès à d'autres ressources pour supporter les opérations et payer les dommages pour la responsabilité potentielle, qui peut être formulée en termes d'un niveau minimum d'actifs nécessaires pour opérer et couvrir les imprévus qui pourraient survenir au sein d'une PKI, par exemple, les actifs sur le bilan d'une organisation, un cautionnement, une lettre de crédit, et un droit en vertu d'un accord pour une indemnité sous certaines circonstances.
- Une déclaration qu'un participant a un programme qui offre une assurance de première partie ou la protection de garantie à d'autres participants dans le cadre de leur utilisation de la PKI.

9.3 Confidentialité des informations de l'entreprise

Ce sous-composant contient les dispositions liées au traitement des information confidentielles de l'entreprise que les participants peuvent communiquer aux autres, tels que les business plan, informations de vente, secrets bancaires, et autres informations reçues d'un tiers de confiance sous un agrément de non-divulgation. spécifiquement, ce sous-composant adresse :

- Le périmètre de ce qui est considéré comme information confidentielle.
- Les types d'informations qui sont considérés hors périmètre des informations confidentielles
- Les responsabilités des participants qui reçoivent des informations confidentielles pour éviter une compromission, et éviter des les utiliser ou les divulguer à des tiers.

9.4 Confidentialité des renseignements personnels

Ce sous-composant est lié à la protection que les participants, particulièrement les CA, RA, et dépôts, peut nécessiter pour permettre d'identifier les informations privées personnelles des candidats de certificat, souscripteurs, et autres participants. Spécifiquement, ce sous-composant adresse les éléments suivant :

- La désignation et divulgation du plan de protection des renseignements personnels applicables qui s'appliquent aux activités des participants, si requis par la stratégie ou la loi applicable.
- Les informations qui sont considérés ou non privée dans la PKI
- Toute responsabilité des participants qui reçoivent des informations privée pour les sécuriser, et éviter leur utilisation ou divulgation à des tiers.
- Tout prérequis pour avis, ou le consentement des individus concernant l'utilisation ou la divulgation d'informations privées.
- Toutes circonstances sous lesquelles un participants a droit ou est tenus de divulguer des informations privées en vertu judiciaire, traitement administratif dans un processus privée ou gouvernemental, ou tout traitement légal.

9.5 Droits de propriété intellectuelle

Ce sou-composant adresse les droits de propriété intellectuelle, tels que les droits d'auteur, brevets, marques, ou secrets commerciaux, que certains participants peuvent avoir ou réclamer dans une CP, CPS, certificats, noms, et clés, ou font l'objet d'une licence ou de participant.

9.6 Représentations et garanties

Ce sous-composant peut inclure des représentations et garanties de divers entités qui sont faites en vertu de la CP ou CPS. Par exemple, une CPS qui sert de contrat peut contenir une garantie de la CA que les informations contenus dans le certificat sont précis. Alternativement, une CPS peut contenir une garantie moins étendue où les informations dans le certificat sont vrai au mieux de la connaissance de la CA après avoir effectué certaines procédures d'authentification de l'identité. Ce sous-composant peut également inclure des prérequis que les représentations et garanties apparaissent dans certains agréments. Par exemple, une CP peut contenir un prérequis qui toutes les CA utilisent un agrément de souscripteur, et qu'un agrément de souscripteur doit contenir une garantie par la CA que les informations dans le certificat est précis. Les participants qui peuvent faire les représentation et garanties incluent les CA, RA, souscripteurs, tiers de confiance, et autres participants.

9.7 exclusions de garanties

Ce sous-composant peut inclure des exclusions de garanties expresses qui pourraient être réputé exister dans un accord, et les exclusions de garanties implicites qui pourraient être imposées par la loi applicable, tels que les garanties de qualité marchande ou d'adéquation pour un but particulier. La CP ou CPS peut directement imposer de tels exclusions, ou la CP ou CPS peut maintenir une obligation que les exclusions apparaissent dans les agrément associés.

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 agrément associés avec la CP ou CPS. Ces limitations peuvent rentrer dans un des deux catégories : les limitations sur les éléments de dommages récupérables et les limitations sur la quantité de dommage récupérable, également connus sous le terme plafonnement de responsabilité. Souvent, les contrats contiennent des clauses empêchant la récupération d'éléments de dommage tels qu'un dommage accessoire et indirect, et les dommage punitifs. Fréquemment, les contrats contiennent des clauses qui limitent la possible récupération d'une partie ou l'autre à un certain montant ou à un montant correspondant à un indice de référence, tels que le montant qu'un vendeur a été payé en vertu du contrat.

9.9 Indémité

Ce sous-composant inclus les dispositions par lesquelles un partie utilise envers un second partie pour les pertes ou dommages encourus par le second partie, résultant généralement de la conduite de la première partie. Ils peuvent apparaîtrent dans une CP, CPS, ou agrément. Par exemple, une CP peut nécessiter que les agréments de souscripteur contiennent un terme sous lequel un souscripteur est responsable de l'indemnisation de la CA pour les pertes que la CA soutient découlant de fausses déclarations d'un souscripteur dans la demande de certificat en vertu de laquelle la CA a émis au souscripteur un certificat inexact. Similairement, une CPS peut dire qu'une CA utilise un agrément de tiers de confiance, sous lequel les tiers de confiance sont responsable de l'indemnisation d'une CA en cas de perte que la CA soutient à cause de l'utilisation d'un certificat sans vérifier les informations de révocation de statut ou l'utilisation d'un certificat dans un but que la CA n'a pas permis.

9.10 Durée et résiliation

Ce sous-composant peut inclure la durée dans laquelle une CP ou CPS demeure en vigueur et les circonstances sous lesquelles le document, portions du document, ou son applicabilité à un participant particulier peut être terminé. En plus ou alternativement, la CP ou CPS peut inclure les exigences que certaines clause de durée et de résiliation apparaissent dans un agrément. En particulier, de tels termes incluent :

- La durée d'un document ou agrément, c'est à dire, quand le document devient effectif et quand il expire s'il n'est pas résilié plus tôt
- Les dispositions de résiliation statuant sur les circonstances sous lesquelles le document, certaines portions, ou son application à un participant particulier cesse d'être en effet.
- Les conséquences de résiliation du document. Par exemple, certaines dispositions d'un agrément peuvent survivre à la résiliation et rester en vigueur. Des exemples incluent la connaissance des droits de propriété intellectuelle et les dispositions de confidentialité. Également, la résiliation peut impliquer une responsabilité des parties de retourner les informations confidentielles au partie qui l'a divulgué.

9.11 Remarques individuels et communications avec les participants

Ce sous-composant discute de la manière par laquelle un participant peut ou doit communiquer avec un autre participant sur une base 1 à 1 pour qu'une telle communication soit légalement effective. Par exemple, une RA peut souhaiter informer la CA qu'elle souhaite terminer sont agrément avec la CA. Ce sous-composant est différent des fonctions de publication et de dépôt, parce contrairement aux communications individuelles décrites dans ce sous-composant, la publication et l'envoi dans un dépôt servent à communiquer à une large audience. Ce sous-composant peut établir des mécanismes pour communiquer et indiquer les informations de contact à utiliser pour router de telles communications, tel que les email signés numériquement à une adresse spécifique, suivie par un email signé d'accusé de réception.

9.12 Modifications

Si sera occasionnellement nécessaire d'amender une CP ou CPS. Certains de ces changements ne vont pas réduire matériellement l'assurance qu'une CP ou son implémentation fournis, et sera jugé par l'administrateur de stratégie sur l'effet insignifiant de l'acceptabilité des certificats. De tels changement dans une CP ou CPS ne nécessitent pas de changement dans l'OID de CP ou le pointeur CPS. D'une autre manière, certains changements dans une spécification va changer matériellement l'acceptabilité des certificats pour des buts spécifiques, et ces changement peuvent nécessiter des changements correspondant à l'OID de la CP ou le pointeur CPS. Ce sous-composant peut également contenir les informations suivantes :

- Les procédures par lesquelles la CP ou CPS et/ou les autres documents doivent, peuvent être, ou sont amendés. Dans le cas des amendements de CP ou CPS, les procédures de changement peuvent inclure un mécanisme de notification pour fournir des avis de modifications proposées aux parties concernées, tels que les souscripteurs ou tiers de confiance, une période de commentaire, un mécanisme par lequel les commentaires sont reçus, revus, et incorporés dans le document, et un mécanisme par lequel les amendements deviennent effectifs.
- Les circonstances sous lesquelles les amendements de CP ou CPS nécessitent un changement d'OID ou pointeur de CPS.

9.13 Procédures de règlement de différends

Ce sous-composant discute des procédures utilisée pour résoudre les différents découlant des CP, CPS et/ou agréments. Des exemples de telles procédures incluent l'exigence qu'un différent soit résolu dans un certain forum ou par des mécanismes de résolutions de différents alternatifs.

9.14 Lois gouvernementales

Ce sous-composant énonce une déclaration que la loi d'une certaine juridiction régit l'interprétation et l'application de la CP ou CPS ou agréments.

9.15 Conformité avec les lois applicables

Ce composant a trait aux conditions énoncées que les participants se conforment avec les lois applicables, par exemple, les lois liées au hardware et software cryptographique que peuvent être sujet aux lois de contrôle d'export d'une juridiction donnée. La CP ou CPS pourrait prétendre imposer de telles exigences ou peuvent exiger que ces dispositions figurent dans d'autres agréments.

9.16 Dispositions diverses

Ce sous-composnat contient diverses dispositions, parfois appelé "dispositions passe-partout" dans les contrats. Les clauses couvertes dans ce sous-composant peuvent apparaître dans une CP, CPS, ou agréments et inclus :

- Une clause d'agrément entière, qui identifie typiquement le document ou les documents comprenant l'intégralité de l'agrément entrée les parties et status que ces agrément remplacent tous les accords antérieurs et actuels écris ou compris oralement relatifs à la même question.
- Une clause de cession, qui peut agir pour limiter la capacité d'un partie dans un agrément, l'attribution de ses droits en vertu de l'accord à un autre partie (comme le droit de recevoir un flux de paiement dans le future) ou de limiter la capacité d'un partie à déléguer ses obligations en vertu de l'accord.
- Une clause de divisibilité, qui énonce les intentions des parties dans le cas où une cour ou un autre tribunal détermine qu'une clause dans un agrément est, pour certaines raisons, invalides ou non-applicables, et dont le but est fréquemment d'empêcher l'inapplicabilité d'une clause causant l'ensemble de l'agrément inapplicable.
- Une clause d'application, qui peut indiquer qu'un partie gagnant dans un litige découlant d'un accord a droit à des honoraires d'avocats dans le cadre de sa récupération, ou peut statuer que le renoncement d'un partie d'une rupture de contrat d'un partie ne constitue par un renoncement permanent, ou un renoncement future ou autres violation de contrat.
- Un clause de force majeur, communément utilisée pour excuser la performance d'un ou plusieurs partie à un accord en raison d'un événement hors du contrôle raisonnable de ou des parties affectées. En règle générale, la durée de l'exécution dispensée est proportionnelle à la durée du retard causé par l'événement. La clause peut également prévoir la résiliation de l'accord dans les circonstances et conditions spécifiées. Les événements considérés pour constituer une force majeur peut inclure ce que l'on appelle les "actes de dieu", les guerres, terrorisme, grèves, catastrophes naturelles, défaillances de fournisseurs ou vendeurs, ou défaillances de l'internet ou autre infrastructure. Les clauses de force majeur doivent être rédigées de manière à être compatibles avec d'autres parties du framework et des agrément de niveau de service applicable. Par exemple, les responsabilités et les capacités de continuation d'activité et de reprise sur incident peut placer des événements sous le contrôle raisonnable des parties, telles qu'une obligation de maintenir une alimentation électrique de secours.

9.17 Autres Dispositions

Ce sous-composant est "fourre-tout" où des responsabilités additionnelles et termes peuvent être imposés aux participants de la PKI qui ne rentre par nécessairement dans une autre catégorie de ce framework. Les rédacteurs de CP et CPS peut placer toute disposition dans ce sous-composant qui n'est pas couvert par un autre sous-composant.

Considérations de sécurité

En accord avec X.509, une stratégie de certificat est un jeu nommé de règles qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou classe d'applications avec des exigences de sécurité particulières. Une CP peut être utilisée par un tiers de confiance pour aider à décider si un certificat, et sa liaison, sont suffisamment dignes de confiance et appropriés à une application particulière.

Le dégré auquel un tier de confiance peut avoir confiance à la liaison embarquée dans un certificat dépend de nombreux facteurs. Ces facteurs peuvent inclure les pratiques suivies par l'autorité de certification en authentifiant le sujet ; la stratégie d'opération de la CA, les procédures, et les contrôles de sécurité techniques, incluant de scope des responsabilités des souscripteurs (par exemple, en protégeant la clé privée), et les responsabilités statué et les termes de responsabilités de la CA (par exemple, les garanties, déclarations de garanties, et les limitations de responsabilité).

Ce document fournis un framework pour adresser les aspects techniques, procédurales, personnelles, et physiques des autorités de certification, d'enregistrement, les dépôts, souscripteurs, et modules cryptographiques de confiance, pour s'assurer que la génération de certificats, la publication, le renouvellement, changement de clé, utilisation, et révocation est faite de manière sécurisée.

Plan d'un jeu de dispositions

Cette section contient un plan recommandé pour un jeu de dispositions prévues pour servir de checklist ou de template standard à utiliser par les rédacteurs de CP ou CPS. Un tel plan facilite :

- La comparaison entre 2 stratégies de certificats durant la cross-certification ou d'autres formes d'interopérations.
- La comparaison d'une CPS avec une CP pour s'assurer que la CPS implémente fidèlement la stratégie
- La comparaison entrée 2 CPS.

Afin de se conformer à cette rfc, les rédacteurs d'une CP ou CPS conformes sont fortement encouragés à adhérer à ce plan. Bien que l'utilisation d'un plan alternatif est découragé, il peut être accepté si une justification est fournie pour la déviation et une table de mappage est fournie pour discerner clairement où chaque éléments décris dans ce plan est fournis.

```
1. INTRODUCTION
1.1 Overview
1.2 Document name and identification
1.3 PKI participants
1.3.1 Certification authorities
1.3.2 Registration authorities
1.3.3 Subscribers
1.3.4 Relying parties
1.3.5 Other participants
1.4 Certificate usage
1.4.1. Appropriate certificate uses
1.4.2 Prohibited certificate uses
1.5 Policy administration
1.5.1 Organization administering the document
1.5.2 Contact person
1.5.3 Person determining CPS suitability for the policy
1.5.4 CPS approval procedures
1.6 Definitions and acronyms
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES
2.1 Repositories
2.2 Publication of certification information
2.3 Time or frequency of publication
2.4 Access controls on repositories
3. IDENTIFICATION AND AUTHENTICATION (11)
3.1 Naming
3.1.1 Types of names
3.1.2 Need for names to be meaningful
3.1.3 Anonymity or pseudonymity of subscribers
```

3.1.4 Rules for interpreting various name forms
3.1.5 Uniqueness of names
3.1.6 Recognition, authentication, and role of trademarks
3.2 Initial identity validation
3.2.1 Method to prove possession of private key
3.2.2 Authentication of organization identity
3.2.3 Authentication of individual identity
3.2.4 Non-verified subscriber information
3.2.5 Validation of authority
3.2.6 Criteria for interoperation
3.3 Identification and authentication for re-key requests
3.3.1 Identification and authentication for routine re-key
3.3.2 Identification and authentication for re-key after revocation
3.4 Identification and authentication for revocation request
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)
4.1 Certificate Application
4.1.1 Who can submit a certificate application
4.1.2 Enrollment process and responsibilities
4.2 Certificate application processing
4.2.1 Performing identification and authentication functions
4.2.2 Approval or rejection of certificate applications
4.2.3 Time to process certificate applications
4.3 Certificate issuance
4.3.1 CA actions during certificate issuance
4.3.2 Notification to subscriber by the CA of issuance of certificate
4.4 Certificate acceptance
4.4.1 Conduct constituting certificate acceptance
4.4.2 Publication of the certificate by the CA
4.4.3 Notification of certificate issuance by the CA to other entities
4.5 Key pair and certificate usage
4.5.1 Subscriber private key and certificate usage
4.5.2 Relying party public key and certificate usage
4.6 Certificate renewal
4.6.1 Circumstance for certificate renewal
4.6.2 Who may request renewal
4.6.3 Processing certificate renewal requests
4.6.4 Notification of new certificate issuance to subscriber
4.6.5 Conduct constituting acceptance of a renewal certificate
4.6.6 Publication of the renewal certificate by the CA
4.6.7 Notification of certificate issuance by the CA to other entities
4.7 Certificate re-key
4.7.1 Circumstance for certificate re-key
4.7.2 Who may request certification of a new public key
4.7.3 Processing certificate re-keying requests
4.7.4 Notification of new certificate issuance to subscriber
4.7.5 Conduct constituting acceptance of a re-keyed certificate
4.7.6 Publication of the re-keyed certificate by the CA
4.7.7 Notification of certificate issuance by the CA to other entities
4.8 Certificate modification
4.8.1 Circumstance for certificate modification
4.8.2 Who may request certificate modification
4.8.3 Processing certificate modification requests
4.8.4 Notification of new certificate issuance to subscriber
4.8.5 Conduct constituting acceptance of modified certificate
4.8.6 Publication of the modified certificate by the CA
4.8.7 Notification of certificate issuance by the CA to other entities
4.9 Certificate revocation and suspension
4.9.1 Circumstances for revocation
4.9.2 Who can request revocation

5.5.4 Archive backup procedures
5.5.5 Requirements for time-stamping of records
5.5.6 Archive collection system (internal or external)
5.5.7 Procedures to obtain and verify archive information
5.6 Key changeover
5.7 Compromise and disaster recovery
5.7.1 Incident and compromise handling procedures
5.7.2 Computing resources, software, and/or data are corrupted
5.7.3 Entity private key compromise procedures
5.7.4 Business continuity capabilities after a disaster
5.8 CA or RA termination
6. TECHNICAL SECURITY CONTROLS (11)
6.1 Key pair generation and installation
6.1.1 Key pair generation
6.1.2 Private key delivery to subscriber
6.1.3 Public key delivery to certificate issuer
6.1.4 CA public key delivery to relying parties
6.1.5 Key sizes
6.1.6 Public key parameters generation and quality checking
6.1.7 Key usage purposes (as per X.509 v3 key usage field)
6.2 Private Key Protection and Cryptographic Module Engineering Controls
6.2.1 Cryptographic module standards and controls
6.2.2 Private key (n out of m) multi-person control
6.2.3 Private key escrow
6.2.4 Private key backup
6.2.5 Private key archival
6.2.6 Private key transfer into or from a cryptographic module
6.2.7 Private key storage on cryptographic module
6.2.8 Method of activating private key
6.2.9 Method of deactivating private key
6.2.10 Method of destroying private key
6.2.11 Cryptographic Module Rating
6.3 Other aspects of key pair management
6.3.1 Public key archival
6.3.2 Certificate operational periods and key pair usage periods
6.4 Activation data
6.4.1 Activation data generation and installation
6.4.2 Activation data protection
6.4.3 Other aspects of activation data
6.5 Computer security controls
6.5.1 Specific computer security technical requirements
6.5.2 Computer security rating
6.6 Life cycle technical controls
6.6.1 System development controls
6.6.2 Security management controls
6.6.3 Life cycle security controls
6.7 Network security controls
6.8 Time-stamping
7. CERTIFICATE, CRL, AND OCSP PROFILES
7.1 Certificate profile
7.1.1 Version number(s)
7.1.2 Certificate extensions
7.1.3 Algorithm object identifiers
7.1.4 Name forms
7.1.5 Name constraints
7.1.6 Certificate policy object identifier
7.1.7 Usage of Policy Constraints extension
7.1.8 Policy qualifiers syntax and semantics
7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL profile
7.2.1 Version number(s)
7.2.2 CRL and CRL entry extensions
7.3 OCSP profile
7.3.1 Version number(s)
7.3.2 OCSP extensions
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
8.1 Frequency or circumstances of assessment
8.2 Identity/qualifications of assessor
8.3 Assessor's relationship to assessed entity
8.4 Topics covered by assessment
8.5 Actions taken as a result of deficiency
8.6 Communication of results
9. OTHER BUSINESS AND LEGAL MATTERS
9.1 Fees
9.1.1 Certificate issuance or renewal fees
9.1.2 Certificate access fees
9.1.3 Revocation or status information access fees
9.1.4 Fees for other services
9.1.5 Refund policy
9.2 Financial responsibility
9.2.1 Insurance coverage
9.2.2 Other assets
9.2.3 Insurance or warranty coverage for end-entities
9.3 Confidentiality of business information
9.3.1 Scope of confidential information
9.3.2 Information not within the scope of confidential information
9.3.3 Responsibility to protect confidential information
9.4 Privacy of personal information
9.4.1 Privacy plan
9.4.2 Information treated as private
9.4.3 Information not deemed private
9.4.4 Responsibility to protect private information
9.4.5 Notice and consent to use private information
9.4.6 Disclosure pursuant to judicial or administrative process
9.4.7 Other information disclosure circumstances
9.5 Intellectual property rights
9.6 Representations and warranties
9.6.1 CA representations and warranties
9.6.2 RA representations and warranties
9.6.3 Subscriber representations and warranties
9.6.4 Relying party representations and warranties
9.6.5 Representations and warranties of other participants
9.7 Disclaimers of warranties
9.8 Limitations of liability
9.9 Indemnities
9.10 Term and termination
9.10.1 Term
9.10.2 Termination
9.10.3 Effect of termination and survival
9.11 Individual notices and communications with participants
9.12 Amendments
9.12.1 Procedure for amendment
9.12.2 Notification mechanism and period
9.12.3 Circumstances under which OID must be changed
9.13 Dispute resolution provisions
9.14 Governing law
9.15 Compliance with applicable law
9.16 Miscellaneous provisions

9.16.1 Entire agreement
9.16.2 Assignment
9.16.3 Severability
9.16.4 Enforcement (attorneys' fees and waiver of rights)
9.16.5 Force Majeure
9.17 Other provisions