rfc3739

Profile de certificats qualifiés

Ce document forme un profile de certificat, basé sur la rfc3280, pour les certificat d'identité émis à des personnes naturelles.

Le profile définis les conventions spécifiques pour les certificats qui sont qualifiés avec un framework définis, les Certificat Qualifiés nommés. Cependant, le profile ne définis aucune exigence légale pour de tels certificats qualifiés.

Le but de ce document est de définir un profile de certificat qui supporte l'émission de certificat qualifiés indépendamment des exigences légales. Le profile n'est cependant pas limité aux certificats qualifiés et le profile peut simplifier les besoins locaux.

Cette spécification fait partie d'une famille de standards pour la PKI X.509 de l'Internet. Elle est basées sur X.509 et la rfc3280, qui définissent les formats de certificat sous-jacent nécessaire à l'implémentation complète de ce standard.

Exigences et hypothèses

Ce terme "Qualified Certificate" est utilisé par la directive européenne pour les signature électroniques (EU-ESDIR) pour référer à un type spécifique de certificats, en conformité avec la législation européenne sur la signature électronique. Cette spécification est prévue pour supporter cette classe de certificats, mais son périmètre n'est pas limité à cette application.

Dans ce standard, le terme "Qualified Certificate" est utilisé généralement, décrivant un certificat dont le but premier est d'identifier une personne avec un haut niveau d'assurance, où le certificat répond à des exigences de qualification définie par un framework légale applicable, tels que la directive européenne sur la signature électronique. Les mécanismes actuels qui décident si un certificat devrait ou non être considéré comme certificat qualifié au regard de la législation est hors du périmètre de ce standard.

L'harmonisation dans le champs des certificats d'identité émis aux personnes naturelles, en particulier les certificats qualifiés, est essentiel dans de nombreux aspects qui sont hors du périmètre de la rfc3280. Les aspects les plus important qui affectent le périmètre de cette spécification sont :

- Définition des noms et informations d'identité pour pouvoir identifier le sujet associé d'une manière uniforme
- Définition des informations qui identifient la CA et la juridiction sous laquelle la CA opère en émettant un certificat particulier.
- Définition de l'extension d'utilisation de clé pour les certificats qualifiés
- Définition de la structure d'informations pour le stockage d'informations biométriques.
- Définition d'une méthode standardisée de stocker des états pré-définis d'intérêt pour des certificats qualifiés.
- Exigences pour les extensions critiques

Propriétés

Ce profile adapte les besoins de profilage pour les certificats qualifiés basés sur les hypothèses que :

- Les certificats qualifiés sont émis par une CA qui qui déclare que le certificat sert le but d'un certificat qualifié
- Le certificat qualifié indique une stratégie de certificat conforme aux engagements, pratiques, et procédures entrepris par la CA.
- Le certificat qualifié est émis à une personne naturelle.
- Le certificat qualifié contient un nom qui peut être soit basé sur le vrai nom du sujet ou un pseudonyme.

Déclaration d'intention

Ce profile définis les conventions pour déclarer dans un certificat qu'il sert l'objectif d'être un certificat qualifié. Cela permet à la CA de définir explicitement cette intention.

Ce profile définis 2 méthodes pour inclure cette information :

- Comme information définie par une stratégie de certificat inclue dans l'extension de stratégies de certificat
- Comme déclaration inclue dans l'extension de déclaration de certificats qualifiés.

problématique de stratégie

Certains aspects de stratégie définissent le contexte dans lequel ce profile est compris et utilisé. Il est cependant en dehors du scope de ce profile de spécifier une stratégie ou les aspects légaux qui vont gouverner les services qui émettent ou utilisent les certificat en accord avec ce profile.

C'est cependant un hypothèse sous-jacente dans ce profile qu'une CA émettrice responsable va entreprendre de suivre une stratégie de certificat qui est consistante avec ses engagements, pratiques et procédure.

Unicité des noms

Les noms distincts sont initialement définis dans X.501 comme représentation d'un nom d'annuaire, définis comme une construction qui identifie un objet particulier parmi un ensemble de tous les objets. Le nom distinct doit être unique pour chaque sujet certifié par une CA comme définie par le champ issuer, pour toute la durée de vie d'une CA.

Profile de certificat et d'extensions de certificat

Cette section définis les conventions de profile de certificat. Le profile est basé sur le profile de certificat de l'Internet (rfc3280), qui lui-même est basé sur le format X.509v3. Pour une implémentation complète de cette section, les implémenteurs doivent consulter les formats et sémantiques définies dans la rfc3280.

Champs de certificat de base

Cette section fournis des détails au regard du contenu de 2 champs dans le certificat de base. Ces champs sont issuer et subject.

Issuer

Le champ issuer devrait identifier l'organisation responsable de l'émission du certificat. Le nom devrait être un nom officiellement enregistré de l'organisation.

Le nom distinct de l'émetteur devrait être spécifié en utilisant le sous-jeu approprié les attributs suivants :

domainComponent

countryName
stateOrProvinceName
organizationName
localityName
serialNumber

L'attribut domainComponent est définis dans la rfc2247, tous les autres attributs sont définis dans la rfc3280 et X.520.

Des attributs additionnels peuvent être présent, mais ils ne doivent pas être nécessaires pour identifier l'organisation émettrice.

Un tiers de confiance peut avoir à consulter les stratégies de certificat associés et/ou la CPS de l'émetteur, pour pouvoir déterminer les sémantiques du nom des champs.

Subject

Le champs subject d'un certificats conforme avec ce profile devrait contenir un nom distinct du sujet. Le champ subject devrait contenir un sous-jeu des attributs suivants :

domainComponent
countryName
commonName
surname
givenName
pseudonym
serialNumber
title
organizationName
organizationUnitName
stateOrProvinceName
localityName

Des attributs additionnels peuvent être présent, mais ils ne doivent pas être nécessaires pour distinguer un nom de sujet d'un autre nom de sujet. C'est à dire, les attributs listés ci-dessus sont suffisant pour s'assurer de l'unicité des noms de sujet.

De ces attributs, le champs sujet devrait inclure au moins un des suivants :

Choix I : commonName
Choix II : givenName
Choix III : pseudonym

La valeur de l'attribut countryName spécifie un contexte général dans lequel d'autres attributs sont compris. L'attribut country n'indique pas nécessairement le pays de citoyenneté ou de résidence du sujet, ni n'indique le pays d'émission.

Note : de nombreuses implémentations X.500 nécessitent la présence de countryName dans le DIT. Dans les cas où le nom du sujet, comme spécifié dans le champ subject, spécifie une entrée d'annuaire X.500, l'attribut countryName devrait toujours être présent.

L'attribut commonName devrait, si présent, contenir un nom du sujet. Cela peut être dans le format de présentation préféré du sujet, ou un format préféré par la CA, ou un autre format. Les pseudonymes, surnoms, et noms ayant une orthographe autre que définie par le nom enregistré peut être utilisé. Pour comprendre la nature du nom présenté dans commonName, les applications conformes peuvent avoir à examiner les valeurs présentes des attributs givenName et surname, ou l'attribut pseudonym.

Note : de nombreuses implémentations client pré-supposent la présence de la valeur de l'attribut commonName dans le champ subject et utilisent cette valeur pour afficher le nom du sujet sans regarder la présence de givenName, surname, ou pseudonym.

Les types d'attribut surname et givenName devraient être utilisés dans le champ suject si ni l'attribut commonName ni l'attribut pseudonym n'est présent. Dans les cas où le sujet a seulement givenName, l'attribut surname devrait être omis.

Le type d'attribut pseudonym devrait, si présent, contenir un pseudonyme du sujet. L'utilisation de l'attribut pseudonym ne doit pas être combiné avec l'utilisation de l'attribut surname et/ou givenName.

Le type d'attribut serialNumber devrait, si présent, être utilisé pour différencier entre les noms où le champ subject serait sinon identique. Cet attribut n'a pas de sémantique définie au-delà de s'assurer de l'unicité des noms des sujets. Il peut contenir un nombre ou un code assigné par la CA ou un identifiant assigné par un gouvernement ou une autorité civile. C'est de la responsabilité de la CA de s'assurer que le serialNumber est suffisant à résoudre toute collision du nom du sujet.

Le type d'attribut title devrait, si présent, être utilisé pour stocker une position désignée ou fonction ou sujet dans l'organisation spécifiée par les attributs organisationnelle présent dans le champs subject. L'association entre le titre, le sujet, et l'organisation est au-delà du périmètre de ce document.

Les types d'attribut organizationName et organizationalUnitName, si présents, sont utilisé pour stocker le nom et les informations essentielles d'une organisation avec lequel le sujet est associé. Le type d'association entre l'organisation et le sujet est au-delà du périmètre de ce document.

Les types d'attribut stateOrProvinceName et localityName devraient, si présents, être utilisés pour stocker les information géographiques avec lequel le sujet est associé. Si une valeur organizationName est également présente, les valeurs d'attribut stateOrProvinceName et localityName devraient être associés avec l'organisation spécifiée. Le type d'association entre stateOrProvinceName et localityName et soit le subject ou organizationName est au-delà du périmètre de ce document.

Les implémentations conformes devraient être capable d'interpréter les attributs nommés dans cette section.

Extensions de certificat

Cette section fournis des détails additionnels sur le contenu des 4 extensions de certificats définis dans la rfc3280 : subjectAltName, subjectDirectoryAttributes, certificate policies, et key usage. Cette section définis également 2 extensions additionnelles : informations biométriques et déclaration de certificat qualifié.

Subject Alternative Name

Si l'extension subjectAltName est présent, et qu'elle contient un directoryName, alors le directoryName doit suivre la convention spécifié dans la section subject plus haut dans ce document.

Subject Directory Attributes

L'extension subjectDirectoryAttributes peut être présente et peut contenir des attributs additionnels associés avec le sujet, comme complément aux informations présentes dans le champ subject et l'extension subjectAltName.

Les attributs prévus pour le stockage dans cet extension sont les attributs qui ne font pas partie du nom distinct du sujet, mais qui peuvent être utiles pour d'autres buts (ex : autorisation). Cette extension ne doit pas être marquée critique.

Les implémentations conformes devraient être capable d'interpréter les attributs suivants :

- dateOfBirth
- placeOfBirth
- gender
- countryOfCitizenship
- countryOfResidence

D'autres attributs peuvent être inclus en accord avec les définitions locales.

L'attribut dateOfBirth devrait, si présent, contenir la valeur de la date de naissance du sujet. La manière dans laquelle la date de naissance est associée avec le sujet est hors du périmètre de ce document. La date de naissance est définis au format GeneralizedTime et devrait préciser GMT 12.00.00 (midi) jusqu'à la granularité des secondes, pour empêcher les changements de date accidentels lié aux ajustement de zone. Par exemple, une date de naissance du 27 Septembre 1959 est encodé "19590927120000Z". Une application qui lit un certificat conforme devrait ignorer toute donnée de temps et simplement présenter la date contenue sans ajustement de zone.

L'attribut placeOfBirth devrait, si présent, contenir la valeur du lieu de naissance du sujet. La manière dans laquelle le lieu de naissance est associé avec le sujet est au-delà du périmètre de ce document.

L'attribut gender devrait, si présent, contenir la valeur du genre du sujet. Pour une femme la valeur 'F' ou 'f', et pour un homme la valeur 'M' ou 'm', doivent être utilisés. La manière dont le genre est associé avec le sujet est hors du périmètre de ce document.

L'attribut countryOfCitizenship devrait, si présent, contenir l'identifiant d'au-moins un des pays de citoyenneté du sujet au moment où le certificat a été délivré. Si plus d'un pays est spécifié, chaque pays devrait être spécifié via un attribut countryOfCitizenship séparé. La détermination de la citoyenneté est une question de droit et est hors du périmètre de ce document.

L'attribut countryOfResidence devrait, si présent, contenir la valeur d'au-moins un pays dans lequel le sujet réside. Si plus d'un pays de résidence est spécifié, chaque pays de résidence devrait être spécifié via un attribut countryOfResidence séparé. La détermination de résidence est une question de droit et est hors du périmètre de ce document.

Stratégies de certificat

L'extension de stratégie de certificat devrait être présent et devrait contenir l'identifiant d'au-moins une stratégie de certificat qui reflète les pratiques et procédures utilisées par la CA. L'extension de stratégie de certificat peut être marquée comme critique.

Les informations fournies par l'émetteur statuant le but du certificat, devrait être évident au travers de la stratégie indiquée.

L'extension de stratégie de certificat doit inclure toutes les informations de stratégie nécessaire pour la validation de chemin de certification. Si les déclarations de stratégie connexes sont incluses dans l'extension QCStatements, alors ces déclarations devraient également être contenues dans les stratégies identifiées.

Les stratégies de certificat peuvent être combinées avec tout qualifiant définis dans la rfc3280.

Utilisation de clé

L'extension d'utilisation de clé devrait être présent. Les paramètres d'utilisation de clé devraient être définis en accord avec les définitions de la rfc3280. D'autres exigences sur les paramètres d'utilisation de clé peuvent être définis par stratégie locale et/ou exigences légales. L'extension d'utilisation de clé devrait être marqué critique.

Informations biométriques

Cette section définis une extension optionnelle pour stocker les informations biométriques. Les informations biométriques sont stockés sous la forme d'un hash d'un modèle biométrique.

Le but de cette extension est de fournir un moyen pour l'authentification d'information biométrique. Les informations biométriques qui correspondent au hash stocké ne sont pas stockés dans cette extension, mais l'extension peut inclure une URI (sourceDataUri) qui référence un fichier contenant cette information.

Si inclus, l'URI doit utiliser le schéma http :// ou https ://. Vu que les données d'identification en cours de vérification peuvent elles-même être des information sensibles, ceux qui déploient ce mécanisme peuvent également souhaiter considérer l'utilisation des URI qui ne peuvent pas être facilement liés par des tiers aux identités de ceux dont l'information est en cours de récupération.

L'utilisation de l'option URI assume que le format d'encodage des données du contenu du fichier est déterminé via des moyens au-delà du périmètre de cette spécification, tel que les conventions de nommage de fichier et les méta-données dans le fichier. L'utilisation de cette URI n'implique pas que c'est la seule manière d'accéder à cette information.

Il est recommandé que les informations biométriques dans cette extension soient limitées aux types d'informations utilisable pour la vérification humaine, par ex., lorsque la décision de savoir si l'information est une représentation précise du sujet est effectuée naturellement par une personne. Cela implique une utilisation où les informations biométriques soient représentée par, par exemple, une image affichée par le tiers de confiance, qui peut être utilisé par le tiers de confiance pour améliorer l'identification du sujet.

Cette extension ne doit pas être marquée critique.

```
biometricInfo EXTENSION ::= {
 SYNTAX BiometricSyntax
 IDENTIFIED BY id-pe-biometricInfo }

id-pe-biometricInfo OBJECT IDENTIFIER ::= {id-pe 2}

BiometricSyntax ::= SEQUENCE OF BiometricData

BiometricData ::= SEQUENCE {
 typeOfBiometricData TypeOfBiometricData,
 hashAlgorithm AlgorithmIdentifier,
 biometricDataHash OCTET STRING,
 sourceDataUri IA5String OPTIONAL }

TypeOfBiometricData ::= CHOICE {
 predefinedBiometricType PredefinedBiometricType,
 biometricDataID OBJECT IDENTIFIER }

PredefinedBiometricType ::= INTEGER { picture(0),
 handwritten-signature(1)} (picture|handwritten-signature,...)
```

L'image de type biométrique prédéfinie, si présent, devrait identifier que l'image source est sous la forme d'une image graphique affichable du sujet. Le hash de l'image graphique devrait être calculée sur tout le fichier image référencé.

L'handwritten-signature de type biométrique prédéfinis, si présent, devrait identifier que la source de donnée est sous la forme d'une image graphique affichable de la signature manuscrite du sujet. Le hash de l'image graphique devrait être calculé sur tout le fichier image référencé.

Déclaration de certificat qualifié

Cette section définis une extension optionnelle pour inclure les déclaration de propriétés explicites du certificat.

Chaque déclaration devrait inclure un identifiant d'objet pour la déclaration et peut également inclure une donnée qualifiante optionnelle contenue dans le paramètre statementInfo.

Si le paramètre statementInfo est inclus, alors l'identifiant d'objet de la déclaration devrait définir la syntaxe et devrait définir les sémantiques de ce paramètre. Si l'identifiant d'objet ne définis pas les sémantiques, un tiers de confiance peut avoir à consulter une stratégie de certificat ou CPS pour déterminer les sémantiques exactes.

Cette extension peut être critique ou non. Si l'extension est critique, cela signifie que toutes les déclarations inclues dans l'extension sont considérés comme critique.

```
qcStatements EXTENSION ::= {
 SYNTAX QCStatements
 IDENTIFIED BY id-pe-qcStatements }

- Note: cette extension en permet pas de mixer les déclarations de certificat qualifiés
- critique et non-critique. Soit tout est critique, soit tous sont non-critique.

id-pe-qcStatements OBJECT IDENTIFIER ::= { id-pe 3 }

QCStatements ::= SEQUENCE OF QCStatement
QCStatement ::= SEQUENCE {
 statementId QC-STATEMENT.&Id({SupportedStatements}),
 statementInfo QC-STATEMENT.&Type({SupportedStatements}{@statementId}) OPTIONAL }

SupportedStatements QC-STATEMENT ::= { qcStatement-1,...}
```

Une déclaration approprié pour cette extension peut être une déclaration par l'émetteur que le certificat est émis comme certificat qualifié en accord avec un système légal particulier.

D'autres déclarations appropriés pour cette extension peuvent être des déclaration liées aux juridictions légales applicables dans lequel le certificat est émis. Par exemple, on peut inclure une limite de confiance maximale pour le certificat indiquant les restrictions de la responsabilité de la CA.

Déclaration prédéfinies

La déclaration de certificat (id-qcs-pkixQCSyntax-v1), identifie la conformité avec les exigences définis dans la rfc3039 obsolète. Cet déclaration est fournie pour l'identification des anciens certificats émis en conformité avec la rfc3039. Cette déclaration ne doit pas être inclue dans les certificats émis en accord avec ce profile.

Ce profile inclus une nouvelle déclaration de certificat qualifié (identifié par l'OID id-qcs-pkixQCSyntax-v2), identifiant la conformité avec les exigences définies dans ce profile. Ce profile de certificat qualifié est référé à la version 2.

Cette déclaration identifie la conformité avec les exigences de la rfc3039. Cette déclaration peut optionnellement contenir des informations de sémantique additionnelles comme spécifié plus bas :

```
qcStatement-1 QC-STATEMENT ::= { SYNTAX SemanticsInformation IDENTIFIED BY id-qcs-pkixQCSyntax-v1 }
```

Cette déclaration identifie la conformité avec les exigences définis dans ce profile de certificat qualifié. Cette déclaration peut optionnellement contenir des informations de sémantiques additionnelles comme spécifié plus bas :

```
qcStatement-2 QC-STATEMENT ::= { SYNTAX SemanticsInformation IDENTIFIED BY id-qcs-pkixQCSyntax-v2 }

SemanticsInformation ::= SEQUENCE {
```

```
 semanticsIdentifier OBJECT IDENTIFIER OPTIONAL,
 nameRegistrationAuthorities NameRegistrationAuthorities OPTIONAL }
 (WITH COMPONENTS {..., semanticsIdentifier PRESENT}|
 WITH COMPONENTS {..., nameRegistrationAuthorities PRESENT})

NameRegistrationAuthorities ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

Le composant SemanticsInformation identifié par id-qcs-pkixQCSyntax-v1 peut contenir un identifiant de sémantique et peut identifier un ou plusieurs nom d'autorité d'enregistrement.

Le composant semanticsIdentifier, si présent, devrait contenir un OID, définissant les sémantiques pour les attributs et les noms dans les champs de base du certificat et les extensions. L'OID peut définir les sémantiques pour tout, ou pour un sous-groupe de tous les attributs présents et/ou les noms.

Le composant NameRegistrationAuthorities, si présent, devrait contenir un nom d'une ou plusieurs autorité d'enregistrement, responsable pour l'enregistrement des attributs ou noms associés avec le sujet. L'association entre un nom identifié d'autorité d'enregistrement et les attributs présents peuvent être définis par un OID de sémantique, par une CP ou CPS, ou autre facteurs implicites.

Si une valeur de type SemanticsInformation est présente dans un QCStatement où le composant statementID est mis à id-qcs-pkig-QCSyntax-v1 ou id-qcs-pkix-QCSyntax-v2, alors au moins un des champs semanticsIdentifier ou nameRegistrationAuthorities doit être présent, comme indiqué. Noter que le composant statementInfo ne doit pas être présent dans une valeur QCStatement même si le composant statementID est mis à id-qcs-pkix-QCSyntax-v1 ou id-qcs-pkix-QCSyntax-v2.

Considérations de sécurité

La valeur légale d'une signature numérique qui est validée avec un certificat qualifié dépend hautement de la stratégie gouvernant l'utilisation de la clé privée associée. Le propriétaire de la clé privée, et le tiers de confiance, devraient s'assurer que la clé privée est utilisée uniquement avec le consentement du propriétaire légitime de la clé.

Vu que les clés publiques sont pour une utilisation publique avec des implications légales pour les parties concernées, certaines conditions devraient exister avant qu'une CA émette des certificat comme certificats qualifiés. Les clés privées associées doivent être unique pour le sujet, et doivent être maintenue sous le contrôle exclusif du sujet. C'est à dire, une CA ne devrait pas émettre un certificat qualifié si les moyens d'utiliser une clé privée ne sont pas protégés contre les utilisation non-prévues. Cela implique que la CA ait une certaine connaissance du module cryptographique du sujet.

La CA doit de plus vérifier que la clé publique contenue dans le certificat représente légitimement le sujet.

La CA ne devrait pas émettre de certificats CA avec les extensions de mappage de stratégie indiquant l'acceptation d'une autre stratégie de CA sauf si les conditions sont rencontrées.

En combinant le bit de nonRepudiation dans l'extension d'utilisation de clé avec d'autres bits d'utilisation de clé peut avoir des implication de sécurité en fonction du contexte dans lequel le certificat est utilisé. Les applications validant les signature électronique basés sur de tels certificats devraient déterminer si la combinaison d'utilisation de clé est approprié pour leur utilisation.

La capacité de comparer 2 certificats qualifiés pour déterminer s'ils représentent la même entité physique est dépendante des sémantiques des noms des sujets. Les sémantiques d'une attribut particulier peut être différent pour différent émetteurs. En comparant les noms sans connaître les sémantiques des noms dans ces certificats particulier peut fournir de faux résultats.

Cette spécification est un profile de la rfc3280. Les considérations de sécurité de ce document s'appliquent à cette spécification également.