Groupe de travail Réseau
Request for Comments : 3739
RFC rendue obsolète : 3039
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Santesson, Microsoft
M. Nystrom, RSA Security
T. Polk, NIST
mars 2004

Infrastructure Internet de clé publique X.509 : profil des certificats qualifiés

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document forme un profil de certificat, fondé sur la RFC3280, pour les certificats d'identité produits aux personnes. Le profil définit des conventions spécifiques pour les certificats qui sont qualifiés dans un cadre légal défini, appelés Certificats qualifiés. Cependant, le profil ne définit aucune exigence légale pour de tels certificats qualifiés.
Le but du présent document est de définir un profil de certificat qui prenne en charge une production des certificats qualifiés indépendante des exigences légales locales. Le profil n'est cependant pas limité aux certificats qualifiés et un profilage plus poussé peut faciliter des besoins locaux spécifiques.

Table des Matières

1. Introduction

La présente spécification fait partie d'une famille de normes pour l'infrastructure de clé publique (PKI, *Public Key Infrastructure*) X.509 pour l'Internet. Elle se fonde sur [X.509] et la [RFC3280], qui définissent les formats et la sémantique de certificat sous-jacents nécessaires pour une pleine mise en œuvre de la présente norme.

Ce profil inclut des mécanismes spécifiques destinés à être utilisés avec des certificats qualifiés. Le terme de certificat qualifié et les hypothèses qui affectent la portée du présent document sont précisés à la Section 2.

La Section 3 définit les exigences sur le contenu des informations de certificat. La présente spécification fournit des profils pour deux champs de certificat : producteur et sujet. Il fournit aussi des profils pour quatre extensions de certificat définies dans la RFC 3280 : nom de remplacement de sujet *(subject alternate name)*, attributs de répertoire de sujets *(subject directory attributes)*, politiques de certificat *(certificate policies)*, et usage de clé *(key usage)*, et il définit deux extensions supplémentaires : les informations biométriques et les déclarations de certificat qualifié. Les extensions de certificat sont présentées dans la version 1997 de la notation numéro un de syntaxe abstraite (ASN.1, *Abstract Syntax Notation One*) [X.680], mais conformément à la RFC 3280 la version 1988 du module ASN.1 de l'Appendice A contient toutes les définitions normative (le module 1997 dans l'Appendice A est pour information).

Dans la Section 4, des considérations sur la sécurité sont discutées afin de clarifier le contexte de sécurité dans lequel la norme peut être utilisée.

L'Appendice A contient toutes les structures ASN.1 pertinentes qui n'ont pas déjà été définies dans la RFC 3280. L'Appendice B contient une note sur les attributs. L'Appendice C contient un exemple de certificat.

Les appendices sont suivis (comme l'indique la table des matières) par les références, l'adresse des auteurs, et la déclaration complète des droits de reproduction.

1.1 Changements depuis la RFC3039

La présente spécification rend obsolète la RFC 3039. La présente spécification diffère de la RFC 3039 dans les domaines de base suivants :

* Des précisions rédactionnelles ont été faites aux sections introductives pour montrer que ce profil est généralement applicable à un large type de certificats, même si son objet principal est de faciliter la production de certificats qualifiés.
* Pour s'aligner sur la RFC 3280, on a inclus la prise en charge de domainComponent des attributs titres dans les noms de sujet, et postalAddress n'est plus pris en charge.
* Pour s'aligner sur l'usage réel, la prise en charge de l'attribut titre dans l'extension des attributs de répertoire sujet n'est plus acceptée.
* Pour faciliter une large applicabilité de ce profil, certaines contraintes sur les réglages d'usage de clé dans l'extension d'usage de clé ont été retirées.
* Une nouvelle qc-Statement reflétant cette seconde version du profil a été définie au paragraphe 3.2.6.1. Ce profil rend obsolète la RFC 3039, mais la qc-statement qui reflète la conformité à la RFC 3039 est aussi définie pour la rétro compatibilité.

1.2 Définitions

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Exigences et hypothèses

Le terme "certificat qualifié" *(abrégé en QC ou qc pour qualified certificatedans les attributs)* est utilisé par la Directive européenne sur les signatures électroniques [EU-ESDIR] pour se référer à un type spécifique de certificats, applicable aux législations européennes sur les signatures électroniques. La présente spécification est destinée à prendre en charge cette classe de certificats, mais sa portée ne se limite pas à cette application.

Avec la présente norme, le terme "certificat qualifié" est utilisé de façon générale, pour décrire un certificat dont l'objet principal est d'identifier une personne avec une grande certitude, où le certificat satisfait à des exigences de qualification

définies par un cadre légal applicable, tel que celui de la Directive européenne sur les signatures électroniques [EU-ESDIR]. Les mécanismes réels qui décident si un certificat devrait ou non être considéré comme un "certificat qualifié" à l'égard d'une législation sortent du domaine d'application de la présente norme.

L'harmonisation dans le champ des certificats d'identité produits aux personnes naturelles, en particulier les certificats qualifiés, est essentielle dans plusieurs aspects qui sortent du cadre d'application de la RFC 3280. Les aspects les plus importants qui affectent le domaine d'application de la présente spécification sont :
- la définition des noms et des informations d'identité afin d'identifier le sujet associé d'une façon uniforme,
- la définition des informations qui identifient la CA et la juridiction sous laquelle fonctionne la CA lorsque elle produit un certificat particulier,
- la définition de l'usage d'extension d'usage de clé pour les certificats qualifiés,
- la définition de la structure des informations pour la mémorisation des informations biométriques,
- la définition d'une façon normalisée de mémoriser les déclarations prédéfinies en rapport avec les certificats qualifiés,
- les exigences pour les extensions critiques.

2.1 Propriétés

Le présent profil s'accommode des besoins de profilage pour les certificats qualifiés sur la base des hypothèses suivantes :
- Les certificats qualifiés sont produits par une CA qui fait une déclaration comme quoi le certificat sert de certificat qualifié, comme exposé au paragraphe 2.2.
- Le certificat qualifié indique qu'une politique de certificat cohérente avec les responsabilités, pratiques, et procédures entreprises par la CA, comme discuté au paragraphe 2.3.
- Le certificat qualifié est produit par une personne naturelle (un être humain vivant).
- Le certificat qualifié contient un nom qui peut être fondé sur le nom réel ou un pseudonyme du sujet.

2.2 Déclaration d’objet

Le présent profil définit les conventions à déclarer au sein d'un certificat qu'il sert à être un certificat qualifié. Cela permet à la CA de définir explicitement cette intention.

La fonction de cette déclaration est donc d'aider toute entité concernée à évaluer les risques associés à la création ou l'acceptation de signatures qui sont fondées sur un certificat qualifié.

Ce profil définit deux façons d'inclure ces informations :
- comme informations définies par une politique de certificat incluse dans l'extenstion de politique du certificat, et
- comme une déclaration incluse dans l'extension Déclarations de certificat qualifié.

2.3 Questions de politique

Certains aspects de politique définissent le contexte dans lequel ce profil doit être compris et utilisé. Il sort cependant du domaine d'application du présent profil de spécifier une politique ou des aspects réglementaires qui gouverneraient les services qui produisent ou utilisent des certificats selon ce profil.

Il y a cependant l'hypothèse sous-jacente de ce profil qu'une CA responsable de la production va entreprendre de suivre une politique de certificat qui est cohérente avec ses responsabilités, pratiques, et procédures.

2.4 Unicité des noms

Le nom distinctif est à l'origine défini dans [X.501] comme une représentation d'un nom de répertoire, défini comme une construction qui identifie un objet particulier au sein d'un ensemble de tous les objets. Le nom distinctif DOIT être unique pour chaque entité sujette certifiée par la CA comme défini par le champ Nom du producteur, pour toute la durée de vie de la CA.

3. Profil de certificat et d'extensions de certificat

Ce paragraphe définit les conventions de profilage de certificat. Le profil se fonde sur le profil de certificat Internet de la RFC3280, qui à son tour se fonde sur le format X.509 version 3. Pour une mise en œuvre complète de cette section, il est EXIGÉ des mises en œuvre qu'elles consultent les formats et la sémantique sous-jacentes définies dans la RFC3280.

Les définitions ASN.1 pertinentes pour la présente section qui ne sont pas fournies par la RFC3280, sont données à l'Appendice A.

3.1 Champs de base de certificat

Ce paragraphe donne des détails supplémentaires concernant le contenu de deux champs du certificat de base. Ces champs sont le producteur et le sujet.

3.1.1 Producteur

Le champ Procucteur DEVRA identifier l'organisation responsable de la production du certificat. Le nom DEVRAIT être un nom officiellement enregistré de l'organisation.

Le nom distinctif du producteur DEVRA être spécifié en utilisant un sous ensemble approprié des attributs suivants :
domainComponent *(composant de domaine)* ;
countryName *(nom de pays)* ;
stateOrProvinceName *(nom d'état ou de région)* ;
organizationName *(nom d'organisation)* ;
localityName *(ville)* ; et
serialNumber *(numéro de série)*.

L'attribut domainComponent est défini dans la [RFC2247], tous les autres attributs sont définis dans la [RFC3280] et [X.520].

Des attributs supplémentaires PEUVENT être présents, mais ils NE DEVRAIENT PAS être nécessaires pour identifier l'organisation productrice.

Un consommateur d'assertions PEUT avoir à consulter les politiques de certificat associées et/ou la déclaration de pratique de certification (CPS, *Certification Practice Statement*) du producteur, afin de déterminer la sémantique des champs de nom.

3.1.2 Sujet

Le champ Sujet d'un certificat conforme au présent profil DEVRA contenir un nom distinctif du sujet (voir au paragraphe 2.4 la définition d'un nom distinctif).

Le champ Sujet DEVRA contenir un sous ensemble approprié des attributs suivants : domainComponent *(domaine d'appartenance)* ; countryName *(pays)* ; commonName *(nom courant)* ; surname *(nom propre)* ; givenName *(prénom)* ; pseudonyme; serialNumber *(numéro de série)* ; title *(titre)* ; organizationName *(nom de l'organisation)* ; organizationalUnitName *(nom de département)* ; stateOrProvinceName *(nom d'état ou province)* ; et localityName *(nom de la ville)*.

L'attribut domainComponent est défini dans la [RFC2247], tous les autres attributs sont définis dans la [RFC3280] et dans [X.520].

D'autres attributs PEUVENT aussi être présents ; cependant, l'utilisation d'autres attributs NE DOIT PAS être nécessaire pour distinguer un nom de sujet d'un autre. C'est à dire que les attributs énumérés ci-dessus sont suffisants pour assurer l'unicité des noms de sujet.

Parmi ces attributs, le champ sujet DEVRA inclure au moins un des suivants :
Choix 1 : nom courant
Choix 2 : nom propre
Choix 3 : pseudonyme

La valeur de l'attribut countryName spécifie un contexte général dans lequel d'autres attributs seront compris. L'attribut de pays n'indique pas nécessairement la nationalité ou le pays de résidence du sujet, pas plus qu'il n'indique le pays de production.

Note : De nombreuses mises en œuvre de X.500 exigent la présence d'un countryName dans la DIT. Dans les cas où le nom du sujet, comme spécifié dans le champ Sujet, spécifie une entrée de répertoire public X.500, l'attribut countryName DEVRAIT toujours être présent.

La valeur de l'attribut commonName DEVRA, lorsque elle est présente, contenir un nom du sujet. Cela PEUT être dans le format de présentation préféré du sujet, ou dans un format préféré par la CA, ou un autre format. Les pseudonymes, surnoms, et les noms épelés autrement que comme défini par le nom enregistré PEUVENT être utilisés. 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 pseudonyme.

Note : De nombreuses mises en œuvre de client présupposent la présence de la valeur de l'attribut commonName dans le champ Sujet et utilisent cette valeur pour afficher le nom du sujet, sans considération des valeurs présentes de l'attribut givenName, surname, ou pseudonyme.

Les types d'attribut surname et givenName DEVRONT être utilisés dans le champ Sujet si ni l'attribut commonName ni l'attribut pseudonyme ne sont présents. Si le sujet a seulement un givenName, l'attribut surname DEVRA être omis.

Le type d'attribut pseudonyme DEVRA, si il est présent, contenir un pseudonyme du sujet. L'utilisation de l'atribut pseudonyme NE DOIT PAS être combinée avec celle d'un des attributs surname et/ou givenName.

Le type d'attribut serialNumber DEVRA, lorsque présent, être utilisé pour différencier les noms où le champ Sujet serait autrement identique. Cet attribut n'a pas de sémantique définie au delà d'assurer l'unicité des noms du sujet. Il PEUT contenir un numbre ou un code alloué par la CA ou un identifiant alloué par un gouvernrment ou une autorité civile. Il est de la responsabilité de la CA de s'assurer que le serialNumber est suffisant pour résoudre toutes collisions de nom du sujet.

Le type d'attribut title DEVRA, lorsque présent, être utilisé pour mémoriser une position ou fonction désignée du sujet au sein de l'organisation spécifiée par les attributs organisationnels présents dans le champ Sujet. L'association entre le titre, le sujet, et l'organisation sort du domaine d'application du présent document.

Les types d'attribut organizationName et organizationalUnitName DEVRONT, lorsque présents, être utilisés pour mémoriser le nom et les informations pertinentes d'une organisation à laquelle le sujet est associé. Le type d'association entre l'organisation et le sujet sort du domaine d'application du présent document.

Les types d'attribut stateOrProvinceName et localityName DEVRONT, lorsque présents, être utilisés pour mémoriser des informations géographiques avec lesquelles le sujet est associé. Si une valeur de organizationName est aussi présente, les valeurs d'attribut stateOrProvinceName et localityName DEVRONT alors être associées à l'organisation spécifiée. Le type d'association entre le stateOrProvinceName et le localityName et soit le sujet, soit l'organizationName sort du domaine d'application du présent document.

Les mises en œuvre conformes DEVRONT être capables d'interpréter les attributs désignés dans cette section.

3.2 Extensions de certificat

Ce paragraphe apporte des détails supplémentaires sur le contenu des quatre extensions de certificat définies dans la [RFC3280] : nom de remplacement du sujet, attributs de répertoire de sujet, politiques de certificat, et utilisation de clé. Ce paragraphe définit aussi des extensions supplémentaires : informations biométriques et déclaration de certificat qualifé.

3.2.1 Nom de remplacement du sujet

Si l'extension subjectAltName est présente, et si elle contient un nom directoryName, le directoryName DOIT suivre les conventions spécifiées au paragraphe 3.1.2 du présent profil.

3.2.2 Attributs du répertoire sujet

L'extension subjectDirectoryAttributes PEUT être présente et PEUT contenir des attributs supplémentaires associés au sujet, comme complément des informations présentes dans le champ Sujet et l'extension de nom de sujet de remplacement .

Les attributs convenables pour être mémorisés dans cette extension sont des attributs qui ne font pas partie du nom distinctif du sujet, mais qui PEUVENT quand même être utiles pour d'autres fins (par exemple, autorisation).

Cette extension NE DOIT PAS être marquée comme critique.

Les mises en œuvre conformes DEVRONT être capables d'interpréter les attributs suivants :
dateOfBirth *(date de naissance)* ;
placeOfBirth *(lieu de naissance)* ;
gender *(sexe)* ;
countryOfCitizenship *(nationalité)* ; et
countryOfResidence *(pays de résidence)*.

D'autres attributs PEUVENT être inclus selon les définitions locales.

L'attribut dateOfBirth DEVRA, lorsque présent, contenir la valeur de la date de naissance du sujet. La manière dont la date de naissance est associée au sujet sort du domaine d'application du présent document. La date de naissance est définie dans le format GeneralizedTime et DEVRAIT spécifier GMT 12.00.00 (midi) jusqu'à la granularité de la seconde, afin d'empêcher un changement accidentel de date dû à des ajustements de fuseau horaire. Par exemple, une date de naissance du 27 septembre 1959 est codée "19590927120000Z". Les applications d'analyse de certificat conformes DEVRAIENT ignorer toutes les données horaires et juste présenter la date contenue sans aucun ajustement de fuseau horaire.

L'attribut placeOfBirth DEVRA, lorsque présent, contenir la valeur du lieu de naissance du sujet. La manière dont le lieu de naissance est associée au sujet sort du domaine d'application du présent document.

L'attribut gender DEVRA, lorsque présent, contenir la valeur du genre du sujet. Pour féminin la valeur "F" (ou "f"), et pour masculin la valeur "M" (ou "m"), doivent être utilisées. La manière dont le genre est associé au sujet sort du domaine d'application du présent document.

L'attribut countryOfCitizenship DEVRA, lorsque présent, contenir l'identifiant d'au moins une des nationalités revendiquées par le sujet au moment où le certificat a été produit. Si plus d'une nationalité est spécifiée, chaque nationalité DEVRAIT être spécifiée par un attribut countryOfCitizenship séparé, d'une seule valeur. La détermination de la nationalité est une affaire juridique qui sort du domaine d'application du présent document.

L'attribut countryOfResidence DEVRA, lorsque présent, contenir la valeur d'au moins un pays dans lequel le sujet est résident. Si plus d'un pays de résidence est spécifié, chaque pays de résidence DEVRAIT être spécifié par un attribut countryOfResidence séparé, d'une seule valeur. La détermination de la résidence est une question juridique qui sort du domaine d'application du présent document.

3.2.3 Politiques de certificat

L'extension Politiques de certificat DEVRA être présente et DEVRA contenir l'identifiant d'au moins une politique de certificat qui reflète les pratiques et procédures entreprises par la CA. L'extension Politiques de certificat PEUT être marquée comme critique.

Les informations fournies par le producteur qui déclarent l'objet du certificat, comme exposé au paragraphe 2.2, DEVRAIENT être évidentes au travers des politiques indiquées.

L'extension Politiques de certificat DOIT inclure toutes les informations de politique nécessaires pour la validation du chemin de certification. Si les déclarations relatives à la politique sont incluses dans l'extension QCStatements (voir le paragraphe 3.2.6) ces déclarations DEVRAIENT alors aussi être contenues dans les politiques identifiées.

Les politiques de certificat PEUVENT être combinées avec tout qualificatif défini dans la [RFC3280].

3.2.4 Usage de clé

L'extension Usage de clé DEVRA être présente. Les réglages d'usage de clé DEVRONT être réglés conformément aux définitions de la [RFC3280]. Des exigences supplémentaires d'usage de clé PEUVENT être définies par la politique locale et/ou des exigences réglementaires locales.

L'extension Usage de clé DEVRAIT être marquée comme critique.

3.2.5 Informations biométriques

Ce paragraphe définit une extension FACULTATIVE pour la mémorisation d'informations biométraiques. Les informations biométriques sont mémorisées sous la forme d'un hachage d'un gabarit biométrique.

L'objet de cette extension est de fournir le moyen d'authentifier les informations biométriques. Les informations biométriques qui correspondent au hachage mémorisé ne sont pas mémorisées dans cette extension, mais l'extension PEUT inclure un URI (sourceDataUri) qui fait référence à un fichier qui contient ces informations.

Si il est inclus, l'URI DOIT utiliser le schéma HTTP (http://) de la [RFC2616] ou le schéma HTTPS (https://) de la [RFC2818]. Comme le fait de vérifier l'identification des données peut lui-même être une information sensible, ceux qui déploient ce mécanisme peuvent aussi souhaiter envisager d'utiliser des URI qui ne peuvent pas être aisément liés aux identités de ceux dont les informations ont été restituées par des étrangers.

L'utilisation de l'option URI présuppose que le format de codage des données du contenu du fichier est déterminé par des moyens qui sortent du domaine d'application de la présente spécification, comme des conventions de dénomination de fichier et des métadonnées à l'intérieur du fichier. L'utilisation de cette option d'URI n'implique pas que ce soit la seule façon d'accéder à ces informations.

Il est RECOMMANDÉ que les informations biométriques dans cette extension soient limitées aux types d'informations adaptés à une vérification par l'homme, c'est-à-dire, où la décision sur si les informations sont une représentation pertinente du sujet est naturellement prise par une personne. Cela implique un usage où les informations biométriques sont représentées, par exemple, par une image graphique affichée au consommateur d'assertions, qui PEUT être utilisée par le consommateur d'assertions pour améliorer l'identification du sujet.

Cette extension NE DOIT PAS être marquée comme critique.

```
biometricInfo  EXTENSION ::= {
SYNTAXE          BiometricSyntax
IDENTIFIÉ PAR     id-pe-biometricInfo }

IDENTIFIANT D'OBJET id-pe-biometricInfo  ::= {id-pe 2}

BiometricSyntax ::= SEQUENCE DE BiometricData

BiometricData ::= SEQUENCE {
      typeOfBiometricData  TypeOfBiometricData,
      hashAlgorithm       AlgorithmIdentifier,
      biometricDataHash    CHAINE D'OCTETS,
      sourceDataUri       IA5String FACULTATIF }

TypeOfBiometricData ::= CHOIX {
      predefinedBiometricType    PredefinedBiometricType,
      biometricDataID          IDENTIFIANT D'OBJET }

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

L'image prédéfinie de type biométrique, lorsque présente, DEVRA identifier que l'image de source est sous la forme d'une image graphique affichable du sujet. Le hachage de l'image graphique DEVRA être calculé sur la totalité du fichier d'image référencé.

La signature manuelle de type biométrique prédéfinie, lorsque présente, DEVRA identifier que les données de source sont sous la forme d'une image graphique affichable de la signature manuelle du sujet. Le hachage de l'image graphique DEVRA être calculé sur la totalité du fichier d'image référencé.

3.2.6 Déclaration de certificat qualifié

Ce paragraphe définit une extension FACULTATIVE pour l'inclusion de déclarations qui définissent les propriétés explicites du certificat.

Chaque déclaration DEVRA inclure un identifiant d'objet pour la déclaration et PEUT aussi inclure des données qualifiantes facultatives contenues dans le paramètre statementInfo.

Si le paramètre statementInfo est inclus, l'identifiant d'objet de la déclaration DEVRA alors définir la syntaxe et DEVRAIT définir la sémantique de ce paramètre. Si l'identifiant d'objet ne définit pas la sémantique, un consommateur d'assertions peut

devoir consulter une politique de certificat pertinente ou un CPS pour déterminer la sémantique exacte.

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

```
qcStatements  EXTENSION ::= {
SYNTAXE           QCStatements
IDENTIFIÉE PAR      id-pe-qcStatements }
```

Note : Cette extension ne permet pas de mélanger des déclarations critiques et non critiques de certificat qualifié. Soit toutes les déclarations doivent être critques, soit toutes les déclarations doivent être non critiques.

```
IDENTIFIANT D'OBJET id-pe-qcStatements ::= { id-pe 3 }
QCStatements ::= SEQUENCE DE QCStatement
QCStatement ::= SEQUENCE {
        statementId   QC-STATEMENT.&Id({SupportedStatements}),
        statementInfo QC-STATEMENT.&Type
        ({SupportedStatements}{@statementId}) FACULTATIF }
    SupportedStatements QC-STATEMENT ::= { qcStatement-1,...}
```

Une déclaration qu'il conviendrait d'inclure dans cette extension PEUT être une déclaration du producteur que le certificat est produit comme certificat qualifié en conformité avec un système juridique particulier (comme exposé au paragraphe 2.2).

D'autres déclarations qu'il conviendrait d'inclure dans cette extension PEUVENT être des déclarations relatives aux jurisdictions compétentes dans lesquelles le certificat est produit. Par exemple, cela PEUT inclure une limite maximum de confiance pour le certificat qui indique des restrictions à la responsabilité de la CA.

3.2.6.1 Déclarations prédéfinies

La déclaration de certificat (id-qcs-pkixQCSyntax-v1) identifie la conformité aux exigences définies dans la RFC obsolète RFC 3039 (version 1). Cette déclaration est donc fournie pour l'identification de vieux certificats produits en conformité à la RFC3039. Cette déclaration NE DOIT PAS être incluse dans les certificats produits conformément au présent profil.

Le présent profil inclut une nouvelle déclaration de certificat qualifié (identifié par l'OID id-qcs-pkixQCSyntax-v2), qui identifie la conformité aux exigences définies dans le présent profil. Ce profil de certificat qualifié est appelé version 2, tandis que celui de la RFC3039 est appelé version 1.

```
qcStatement-1 QC-STATEMENT ::= { SYNTAXE SemanticsInformation IDENTIFIÉE PAR id-qcs-pkixQCSyntax-v1 }
-- Cette déclaration identifie la conformité aux exigences de la RFC3039 (Version 1). Cette déclaration peut facultativement
contenir des informations de sémantique supplémentaires comme spécifié ci-dessous.

qcStatement-2 QC-STATEMENT ::= { SYNTAXE SemanticsInformation IDENTIFIÉ PAR id-qcs-pkixQCSyntax-v2 }
-- Cette déclaration identifie la conformité aux exigences définies dans le présent profil de certificat qualifié (Version 2). Cette
déclaration peut facultativement contenir des informations de sémantique supplémentaires comme spécifié ci-dessous.

SemanticsInformation ::= SEQUENCE {
IDENTIFIANT D'OBJET       semanticsIdentifier FACULTATIF,
        nameRegistrationAuthorities NameRegistrationAuthorities    FACULTATIF }
        (AVEC COMPOSANTS {..., semanticsIdentifier PRESENT}|
         AVEC COMPOSANTS {..., nameRegistrationAuthorities PRESENT})

NameRegistrationAuthorities ::=  SEQUENCE TAILLE (1..MAX) DE GeneralName
```

Le composant SementicsInformation identifié par id-qcs-pkixQCSyntax-v1 PEUT contenir un identifiant sémantique et PEUT identifier une ou plusieurs autorités d'enregistrement de nom.

Le composant semanticsIdentifier, si il est présent, DEVRA contenir un OID, définissant la sémantique des attributs et noms dans les champs de base de certificat et les extensions de certificat. L'OID peut définir la sémantique de tous les attributs et/ou noms présents ou d'un sous groupe d'entre eux.

Le composant NameRegistrationAuthorities, si il est présent, DEVRA contenir un nom d'une ou plusieurs autorités d'enregistrement de nom, responsables de l'enregistrement des attributs ou noms associés au sujet. L'association entre une

autorité d'enregistrement de nom identifiée et les attributs présents PEUT être définie par un OID identifiant de sémantique, par une politique de certificat (ou CPS), ou d'autres facteurs implicites.

Si une valeur de type SemanticsInformation est présente dans une QCStatement où le composant statementID est réglé à id-qcs-pkix-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 n'a pas besoin d'être présent dans une valeur de QCStatement même si le composant statementID est réglé à id-qcs-pkix-QCSyntax-v1 ou id-qcs-pkix-QCSyntax-v2.

4. Considérations pour la sécurité

La valeur légale d'une signature numérique qui est validée par un certificat qualifié va dépendre étroitement de la politique qui gouverne l'utilisation de la clé privée associée. Le détenteur de la clé privée, aussi bien que le consommateur d'assertions, devraient tous deux s'assurer que la clé privée n'est utilisée qu'avec le consentement du détenteur légitime de la clé.

Comme les clés publiques sont pour usage public avec des implications légales pour les parties, certaines conditions devraient exister avant que les CA produisent des certificats comme certificats qualifiés. Les clés privées associées doivent être uniques pour le sujet, et doivent être entretenues sous le seul contrôle du sujet. C'est-à-dire qu'une CA ne devrait pas produire un certificat qualifié si les moyens d'utiliser la clé privée ne sont pas protégés contre un usage non prévu. Cela implique que la CA a connaissance du module cryptographique du sujet.

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

Les CA ne devraient pas produire de certificats de CA avec des extensions de transposition de politique qui indiquent l'acceptation de la politique d'une autre CA sauf si ces conditions sont satisfaites.

La combinaison du bit de non répudiation dans l'extension de certificat keyUsage avec d'autres bits de keyUsage peut avoir des implications sur la sécurité selon le contexte dans lequel le certificat va être utilisé. Les applications qui valident des signatures électroniques sur la base de tels certificats devraient déterminer si la présente combinaison d'usage de clé est appropriée pour leur utilisation.

La capacité à comparer deux certificats qualifiés pour déterminer si ils représentent la même entité physique dépend de la sémantique des noms des sujets. La sémantique d'un attribut particulier peut être différente pour des producteurs différents. Comparer des noms sans connaître la sémantique des noms dans ces certificats particuliers peut conduire à des résultats trompeurs.

La présente spécification est un profil de la RFC 3280. La section des considérations sur la sécurité de ce document s'applique aussi à la présente spécification.

A. Définitions ASN.1

Comme dans la RFC3280, les modules ASN.1 sont fournis selon deux variantes différentes de la syntaxe ASN.1.

L'Appendice A.1 est dans la syntaxe 1988, et n'utilise pas de macros. Cependant, comme le module importe des définitions de type des modules de la RFC3280 qui ne sont pas complètement dans la syntaxe 1988, le même commentaire que dans la RFC3280 concernant son utilisation s'applique ici aussi ; c'est-à-dire, l'Appendice A.1 peut être analysé par un analyseur ASN.1 1988 en retirant les définitions pour les types UNIVERSAL et toutes les références à eux dans les modules 1988 de la RFC3280.

L'Appendice A.2 est dans la syntaxe 1997.

En cas de discordances entre ces modules, le module 1988 est le module normatif.

A.1 Module ASN.1 1988 (normatif)

```
PKIXqualified88 {iso(1) identified-organization(3) dod(6)
   internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
   id-mod-qualified-cert(31) }
```

```
ETIQUETTES EXPLICITES DE DEFINITIONS ::=

  DEBUT

-- EXPORTE TOUT --

  IMPORTE

GeneralName
   DE PKIX1Implicit88 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-
pkix1-implicit(19)}

AlgorithmIdentifier, DirectoryString, AttributeType, id-pkix, id-pe
   DE PKIX1Explicit88 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-
pkix1-explicit(18)};

-- OID définis en local

-- Arc pour attributs de certificat qualifié de données personnelles
IDENTIFIANT D'OBJET  id-pda   ::= { id-pkix 9 }

  -- Arc for QC statements
IDENTIFIANT D'OBJET id-qcs  OBJECT IDENTIFIER ::= { id-pkix 11 }

  -- Personal data attributes

  id-pda-dateOfBirth        AttributeType ::= { id-pda 1 }
  DateOfBirth ::=           GeneralizedTime

  id-pda-placeOfBirth       AttributeType ::= { id-pda 2 }
  PlaceOfBirth ::=          DirectoryString

  id-pda-gender             AttributeType ::= { id-pda 3 }
  Gender ::=                PrintableString (SIZE(1))
                        -- "M", "F", "m" or "f"

  id-pda-countryOfCitizenship AttributeType ::= { id-pda 4 }
  CountryOfCitizenship ::=    PrintableString (SIZE (2))
                        -- ISO 3166 Country Code

  id-pda-countryOfResidence   AttributeType ::= { id-pda 5 }
  CountryOfResidence ::=      PrintableString (SIZE (2))
                        -- ISO 3166 Country Code

  -- Certificate extensions

  -- Biometric info extension

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

IDENTIFIANT D'OBJET BiometricSyntax ::= SEQUENCE OF BiometricData

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

  TypeOfBiometricData ::= CHOICE {
     predefinedBiometricType   PredefinedBiometricType,
     biometricDataOid          IDENTIFIANT D'OBJET }
```

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

  -- QC Statements Extension
  -- NOTE: Cette extension does not allow to mix critical and
  -- non-critical certificat qualifié Statements. Either all
  -- statements must be critical or all statements must be
  -- non-critical.

IDENTIFIANT D'OBJET id-pe-qcStatements OBJECT IDENTIFIER ::= { id-pe 3}

  QCStatements ::= SEQUENCE OF QCStatement

  QCStatement ::= SEQUENCE {
     statementId       IDENTIFIANT D'OBJET,
     statementInfo      ANY DEFINED BY statementId FACULTATIF}

  -- QC statements
IDENTIFIANT D'OBJET id-qcs-pkixQCSyntax-v1   IDENTIFIANT D'OBJET ::= { id-qcs 1 }
  --  This statement identifies conformance with requirements
  --  defined in RFC 3039 (Version 1). This statement may
  --  optionally contain additional semantics information as specified
  --  below.

IDENTIFIANT D'OBJET id-qcs-pkixQCSyntax-v2  ::= { id-qcs 2 }
-- Cette déclaration identifie la conformité aux exigences définies dans ce profil de certificat qualifié (version 2). Cette
déclaration peut facultativement contenir des onformations sémantiques supplémentaires, comme spécifié ci-dessous.

SemanticsInformation  ::= SEQUENCE {
     semanticsIndentifier       IDENTIFIANT D'OBJET FACULTATIF,
     nameRegistrationAuthorities NameRegistrationAuthorities FACULTATIF
     } – Au moins un champ doit être présent.

NameRegistrationAuthorities ::= SEQUENCE TAILLE (1..MAX) DE GeneralName

FIN
```

A.2 Module ASN.1 1997 (pour information)

```
PKIXqualified97 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-
qualified-cert-97(35) }

ETIQUETTES EXPLICITES DE DEFINITIONS ::=

DEBUT

-- EXPORTE TOUT --

IMPORTE

informationFramework, certificateExtensions, selectedAttributeTypes, authenticationFramework, upperBounds, id-at
     DE UsefulDefinitions {joint-iso-itu-t(2) ds(5) module(1) usefulDefinitions(0) 3 }

ub-name
     DE UpperBounds upperBounds

GeneralName
     DE CertificateExtensions certificateExtensions

ATTRIBUTE, AttributeType
```

```
        DE InformationFramework informationFramework

    DirectoryString
        DE SelectedAttributeTypes selectedAttributeTypes

    AlgorithmIdentifier, Extension, EXTENSION
        DE AuthenticationFramework authenticationFramework

    id-pkix, id-pe
        DE PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
        id-pkix1-explicit(18) };

    -- OID définis en local

    -- Arc pour les attributs de données personelles de certificat qualifié
    IDENTIFIANT D'OBJET id-pda ::= { id-pkix 9 }

    -- Arc pour les déclarations de certificat qualifié
    IDENTIFIANT D'OBJET id-qcs ::= { id-pkix 11 }

    -- Attributs de données personnelles

    id-pda-dateOfBirth              AttributeType ::= { id-pda 1 }
    id-pda-placeOfBirth             AttributeType ::= { id-pda 2 }
    id-pda-gender                   AttributeType ::= { id-pda 3 }
    id-pda-countryOfCitizenship     AttributeType ::= { id-pda 4 }
    id-pda-countryOfResidence       AttributeType ::= { id-pda 5 }

    -- Extensions de certificat

    IDENTIFIANT D'OBJET id-pe-biometricInfo ::= { id-pe 2 }
    IDENTIFIANT D'OBJET id-pe-qcStatements ::= { id-pe 3 }

    -- Déclarations de certificat qualifié

    IDENTIFIANT D'OBJET id-qcs-pkixQCSyntax-v1 ::= { id-qcs 1 }
    IDENTIFIANT D'OBJET id-qcs-pkixQCSyntax-v2 ::= { id-qcs 2 }

    -- Attributs de données personnelles

    dateOfBirth ATTRIBUT ::= {
        AVEC SYNTAXE GeneralizedTime
        ID      id-pda-dateOfBirth }

    placeOfBirth ATTRIBUT ::= {
        AVEC SYNTAXE DirectoryString {ub-name}
        ID      id-pda-placeOfBirth }

    gender ATTRIBUT ::= {
        AVEC SYNTAXE PrintableString (TAILLE(1) ^ DE("M"|"F"|"m"|"f"))
        ID      id-pda-gender }

    countryOfCitizenship ATTRIBUT ::= {
        AVEC SYNTAXE PrintableString (TAILLE (2))
            (CONTRAINT PAR { -- seulement codes ISO 3166 -- })
        ID      id-pda-countryOfCitizenship }

    countryOfResidence ATTRIBUT ::= {
        AVEC SYNTAXE PrintableString (TAILLE (2))
            (CONTRAINT PAR { -- seulement codes ISO 3166 -- })
        ID      id-pda-countryOfResidence }

    -- Extensions de certificat
```

```
-- Extension d'informations biométriques

biometricInfo  EXTENSION ::= {
      SYNTAXE          BiometricSyntax
      IDENTIFIE PAR      id-pe-biometricInfo }

BiometricSyntax ::= SEQUENCE DE BiometricData

BiometricData ::= SEQUENCE {
      typeOfBiometricData TypeOfBiometricData,
      hashAlgorithm       AlgorithmIdentifier,
      biometricDataHash   CHAINE D'OCTETS,
      sourceDataUri       IA5String FACULTATIF,
      ... -- Pour de futures extensions -- }

TypeOfBiometricData ::= CHOIX {
      predefinedBiometricType PredefinedBiometricType,

IDENTIFIANT D'OBJET  biometricDataOid   }

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

-- Extension de déclaration de certificat qualifié
-- Note : Cette extension ne permet pas de mélanger des déclarations de certificat qualifié critiques et non critiques. Soit toutes
les déclarations sont critiques, soit toutes les déclarations sont non critiques.

qcStatements  EXTENSION ::= {
      SYNTAXE       QCStatements
      IDENTIFIE PAR id-pe-qcStatements }

QCStatements ::= SEQUENCE DE QCStatement

QCStatement ::= SEQUENCE {
      statementId   QC-STATEMENT.&id({SupportedStatements}),
      statementInfo QC-STATEMENT.&Type
      ({SupportedStatements}{@statementId}) FACULTATIF }

QC-STATEMENT ::= CLASSE {
      &id   IDENTIFIANT D'OBJET UNIQUE,
      &Type FACULTATIF }
      AVEC SYNTAXE {
      [SYNTAXE &Type] IDENTIFIE PAR &id }

qcStatement-1 QC-STATEMENT ::= { SYNTAXE SemanticsInformation
      IDENTIFIE PAR id-qcs-pkixQCSyntax-v1}
-- Cette déclaration identifie la conformité aux exigences définies dans la RFC 3039 (version 1). Cette déclaration peut
facultativement contenir des informations de sémantique supplémentaires, comme spécifié ci-dessous.

qcStatement-2 QC-STATEMENT ::= { SYNTAXE SemanticsInformation
      IDENTIFIE PAR id-qcs-pkixQCSyntax-v2}
-- Cette déclaration identifie la conformité aux exigences définies dans ce profil de certificat qualifié (version 2). Cette
déclaration peut facultativement contenir des informations de sémantique supplémentaires, comme spécifié ci-dessous.

SemanticsInformation ::= SEQUENCE {
      semanticsIdentifier        IDENTIFIANT D'OBJET FACULTATIF,
      nameRegistrationAuthorities NameRegistrationAuthorities FACULTATIF
      }(AVEC COMPONENTS {..., semanticsIdentifier PRESENT}|
        AVEC COMPONENTS {..., nameRegistrationAuthorities PRESENT})

NameRegistrationAuthorities ::= SEQUENCE TAILLE (1..MAX) DE GeneralName
```

-- L'ensemble d''objets d'information suivant est défini pour restreindre l'ensemble des applications d'attributs qu'il est nécessaire de reconnaître comme QCS.

SupportedStatements QC-STATEMENT ::= { qcStatement-1 | qcStatement-2 , ... – pour de futures extensions -- }

FIN

B. Note sur les attributs

Le présent document définit plusieurs nouveaux attributs, à utiliser dans les champs Sujet des certificats produits et dans l'extension sujetDirectoryAttributes. Une définition complète de ces nouveaux attributs (incluant les règles de correspondance) ainsi que les classes d'objets pour les prendre en charge dans les répertoires accessibles par LDAP, se trouve dans PKCS 9 [RFC2985].

C. Exemple de certificat

Ce paragraphe contient la structure ASN.1, un dépôt ASN.1, et le codage en DER d'un certificat produit conformément au présent profil. L'exemple a été développé à l'aide du compilateur ASN.1 OSS. Le certificat a les caractéristiques suivantes :

1. Le certificat est signé avec RSA et l'algorithme de hachage SHA-1.
2. Le nom distinctif du producteur est (en utilisant la syntaxe spécifiée dans la [RFC2253]) : O=GMD - Forschungszentrum Informationstechnik GmbH, C=DE
3. Le nom distinctif du sujet est (en utilisant la syntaxe spécifiée dans la [RFC2253]) : GN=Petra+SN=Barzin, O=GMD - Forschungszentrum Informationstechnik GmbH, C=DE
4. Le certificat a été produit le 1 février 2004 et expirera le 1 février 2008.
5. Le certificat contient une clé RSA de 1024 bits.
6. Le certificat inclut une extension critique d'usage de clé indiquant exclusivement la non répudiation.
7. Le certificat inclut une extension d'identifiant de politique de certificat qui indique les pratiques et procédures entreprises par la CA productrice (identifiant d'objet 1.3.36.8.1.1). L'identifiant d'objet de politique de certificat est défini par TeleTrust, Allemagne.
8. Le certificat inclut une extension d'attributs de répertoire sujet qui contient les attributs suivants :
   date de naissance : 14 octobre 1971
   lieu de naissance : Darmstadt
   nationalité : Allemagne
   sexe : féminin
9. Le certificat inclut une extension de déclaration de certificat qualifié qui indique que le nom de l'autorité d'enregistrement de dénomination est "municipality@darmstadt.de".
10. Le certificat inclut, conformément à la RFC3280, une extension d'identifiant de clé d''autorité.

C.1 Structure ASN.1

C.1.1 Extensions

Comme les extensions sont déjà codées en DER lorsque elles sont placées dans la structure à signer, elle sont, dans un souci de clarté, montrées ici avec la notation de valeur définie dans [X.680].

C.1.1.1 Extension sujetDirectoryAttributes

```
certSubjDirAttrs AttributesSyntax ::= {
   {
      type id-pda-countryOfCitizenship,
      values {
         PrintableString : "DE"
      }
   },
   {
      type id-pda-gender,
      values {
         PrintableString : "F"
```

```
      }
    },
    {
      type id-pda-dateOfBirth,
      values {
        GeneralizedTime : "197110141200Z"
      }
    },
    {

      type id-pda-placeOfBirth,
      values {
        DirectoryString : utf8String : "Darmstadt"
      }
    }
  }
```

C.1.1.2 Extension keyUsage

```
  certKeyUsage KeyUsage ::= {nonRepudiation}
```

C.1.1.3 Extension certificatePolicies

```
  certCertificatePolicies CertificatePoliciesSyntax ::= {
    {
      policyIdentifier {1 3 36 8 1 1}
    }
  }
```

C.1.1.4 Extension qcStatements

```
  certQCStatement QCStatements ::= {
    {
      statementId   id-qcs-pkixQCSyntax-v2,
      statementInfo SemanticsInformation : {
        nameRegistrationAuthorities {
          rfc822Name : "municipality@darmstadt.de"
        }
      }
    }
  }
```

C.1.1.5 Extension authorityKeyIdentifier

```
  certAKI AuthorityKeyIdentifier ::= {
    keyIdentifier '000102030405060708090A0B0C0D0E0FFEDCBA98'H
  }
```

C.1.2. Certificat

La portion signée du certificat est montrée ici avec la notation de valeur définie dans [X.680]. Noter que les valeurs d'extension sont déjà codées en DER dans cette structure. Certaines valeurs ont été tronquées pour des besoins de lisibilité.

```
  certCertInfo CertificateInfo ::= {
    version v3,
    serialNumber 1234567890,

    signature
    {
      algorithm { 1 2 840 113549 1 1 5 },
      parameters RSAParams : NULL
```

```
},
issuer rdnSequence :
 {
  {
   {
    type { 2 5 4 6 },
    value PrintableString : "DE"
   }
  },
  {
   {
    type { 2 5 4 10 },
    value UTF8String :
   }
  }
 },
validity
{
 notBefore utcTime : "040201100000Z",
 notAfter utcTime :  "080201100000Z"
},
sujet rdnSequence :
 {
  {
   {
    type { 2 5 4 6 },
    value PrintableString : "DE"
   }
  },
  {
   {
    type { 2 5 4 10 },
    value UTF8String :
      "GMD Forschungszentrum Informationstechnik GmbH"
   }
  },
  {
   {
    type { 2 5 4 4 },
    value UTF8String : "Barzin"
   },
   {
    type { 2 5 4 42 },
    value UTF8String : "Petra"
   }
  }
 },
sujetPublicKeyInfo
{
 algorithm
 {
  algorithm { 1 2 840 113549 1 1 1 },
  parameters RSAParams : NULL
 },
 sujetPublicKey '30818902818100DCE74CD5...0203010001'H
},
extensions
{
 {
  extnId { 2 5 29 9 },  -- sujetDirectoryAttributes
  extnValue '305B301006082B0601050507090...7374616474'H
 },
 {
```

```
      extnId { 2 5 29 15 }, -- keyUsage
      critical TRUE,
      extnValue '03020640'H
     },
     {
      extnId { 2 5 29 32 }, -- certificatePolicies
      extnValue '3009300706052B24080101'H
     },
     {
      extnId { 2 5 29 35 }, -- authorityKeyIdentifier
      extnValue '30168014000102030405060708090A0B0C0D0E0FFEDCBA98'H
     },
     {
      extnId { 1 3 6 1 5 5 7 1 3 }, -- qcStatements
      extnValue '302B302906082B06010505070B0...4742E6465 'H
     }
    }
   }
```

C.2 Dépôt ASN.1

Ce paragraphe contient un dépôt ASN.1 de la portion signée du certificat. Certaines valeurs ont été tronquées pour la rendre plus lisible.

```
CertificateInfo SEQUENCE: tag = [UNIVERSAL 16] constructed; length = 633
  version : tag = [0] constructed; length = 3
    Version INTEGER: tag = [UNIVERSAL 2] primitive; length = 1
      2

  serialNumber CertificateSerialNumber INTEGER: tag = [UNIVERSAL 2]
  primitive; length = 4
    1234567890
  signature AlgorithmIdentifier SEQUENCE: tag = [UNIVERSAL 16]
  constructed; length = 13
    algorithm OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
    primitive; length = 9
      { 1 2 840 113549 1 1 5 }
    parameters OpenType
      NULL
  issuer Name CHOICE
    rdnSequence RDNSequence SEQUENCE OF: tag = [UNIVERSAL 16]
    constructed; length = 72
      RelativeDistinguishedName SET OF: tag = [UNIVERSAL 17]
      constructed; length = 11
        AttributeTypeAndValue SEQUENCE: tag = [UNIVERSAL 16]
        constructed; length = 9
          type OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
          primitive; length = 3
            { 2 5 4 6 } -- id-at-countryName
          value PrintableString
            "DE"
      RelativeDistinguishedName SET OF: tag = [UNIVERSAL 17]
      constructed; length = 57
        AttributeTypeAndValue SEQUENCE: tag = [UNIVERSAL 16]
        constructed; length = 55
          type OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
          primitive; length = 3
            { 2 5 4 10 } -- id-at-organizationName
          value UTF8String
            "GMD Forschungszentrum Informationstechnik GmbH"
  validity Validity SEQUENCE: tag = [UNIVERSAL 16]
```

```
constructed; length = 30
 notBefore Time CHOICE
  utcTime UTCTime: tag = [UNIVERSAL 23] primitive; length = 13
   040201100000Z
 notAfter Time CHOICE
  utcTime UTCTime: tag = [UNIVERSAL 23] primitive; length = 13
   080201100000Z
sujet Name CHOICE
 rdnSequence RDNSequence SEQUENCE OF: tag = [UNIVERSAL 16]
 constructed; length = 101
  RelativeDistinguishedName SET OF: tag = [UNIVERSAL 17]
  constructed; length = 11
   AttributeTypeAndValue SEQUENCE: tag = [UNIVERSAL 16]
   constructed; length = 9
    type OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
    primitive; length = 3
     { 2 5 4 6 } -- id-at-countryName
    value PrintableString
     "DE"
  RelativeDistinguishedName SET OF: tag = [UNIVERSAL 17]
  constructed; length = 55
   AttributeTypeAndValue SEQUENCE: tag = [UNIVERSAL 16]
   constructed; length = 53
    type OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
    primitive; length = 3
     { 2 5 4 10 } -- id-at-organizationName
    value UTF8String
     "GMD Forschungszentrum Informationstechnik GmbH"
  RelativeDistinguishedName SET OF: tag = [UNIVERSAL 17]
  constructed; length = 29
   AttributeTypeAndValue SEQUENCE: tag = [UNIVERSAL 16]
   constructed; length = 13
    type OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
    primitive; length = 3
     { 2 5 4 4 } -- id-at-surname
    value UTF8String
     "Barzin"
   AttributeTypeAndValue SEQUENCE: tag = [UNIVERSAL 16]
   constructed; length = 12
    type OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
    primitive; length = 3
     { 2 5 4 42 } -- id-at-givenName
    value UTF8String
     "Petra"
sujetPublicKeyInfo SubjectPublicKeyInfo SEQUENCE:
tag = [UNIVERSAL 16] constructed; length = 159
 algorithm AlgorithmIdentifier SEQUENCE: tag = [UNIVERSAL 16]
 constructed; length = 13
  algorithm OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
  primitive; length = 9
   { 1 2 840 113549 1 1 1 } -- rsaEncryption
  parameters OpenType
   NULL
 sujetPublicKey BIT STRING: tag = [UNIVERSAL 3]
 primitive; length = 141
  0x0030818902818100dce74cd5a1d55aeb01cf5ecc20f3c3fca787...
extensions : tag = [3] constructed; length = 233
 Extensions SEQUENCE OF: tag = [UNIVERSAL 16]
 constructed; length = 230
  Extension SEQUENCE: tag = [UNIVERSAL 16]
  constructed; length = 100
   extnId OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
   primitive; length = 3
```

```
    { 2 5 29 9 } -- id-ce-sujetDirectoryAttributes
  extnValue OCTET STRING: tag = [UNIVERSAL 4]
  primitive; length = 93
    0x305b301006082b06010505070904310413024445300f06082...
Extension SEQUENCE: tag = [UNIVERSAL 16]
constructed; length = 14
  extnId OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
    primitive; length = 3
    { 2 5 29 15 } -- id-ce-keyUsage
  critical BOOLEAN: tag = [UNIVERSAL 1] primitive; length = 1
    TRUE
  extnValue OCTET STRING: tag = [UNIVERSAL 4]
  primitive; length = 4
    0x03020640
Extension SEQUENCE: tag = [UNIVERSAL 16]
constructed; length = 18
  extnId OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
  primitive; length = 3
    { 2 5 29 32 } -- id-ce-certificatePolicies
  extnValue OCTET STRING: tag = [UNIVERSAL 4]
  primitive; length = 11
    0x3009300706052b24080101
Extension SEQUENCE: tag = [UNIVERSAL 16]
constructed; length = 31
  extnId OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
  primitive; length = 3
    { 2 5 29 35 } -- id-ce-authorityKeyIdentifier
  extnValue OCTET STRING: tag = [UNIVERSAL 4]
  primitive; length = 24
    0x3016801400010203040506070809 0a0b0c0d0e0ffedcba98
Extension SEQUENCE: tag = [UNIVERSAL 16]
constructed; length = 57
  extnId OBJECT IDENTIFIER: tag = [UNIVERSAL 6]
  primitive; length = 8
    { 1 3 6 1 5 5 7 1 3 } -- id-pe-qcStatements
  extnValue OCTET STRING: tag = [UNIVERSAL 4]
  primitive; length = 45
    0x302b302906082b06010505070b02301d301b81196d756e696...
```

C.3 Codage DER

Ce paragraphe contient le certificat complet, codé en DER, en hexadécimal.

30820310 30820279 A0030201 02020449 9602D230 0D06092A 864886F7 0D01010505003048 310B3009 06035504
06130244 45313930 37060355 040A0C30 474D44202D20466F 72736368 756E6773 7A656E74 72756D20 496E666F
726D6174 696F6E7374656368 6E696B20 476D6248 301E170D 30343032 30313130 30303030 5A170D3038303230
31313030 3030305A 3065310B 30090603 55040613 02444531 373035060355040A 0C2E474D 4420466F 72736368
756E6773 7A656E74 72756D20 496E666F726D6174 696F6E73 74656368 6E696B20 476D6248 311D300C 06035504
2A0C055065747261 300D0603 5504040C 06426172 7A696E30 819F300D 06092A86 4886F70D01010105 0003818D
00308189 02818100 DCE74CD5 A1D55AEB 01CF5ECC 20F3C3FCA787CFCB 571A21AA 8A20AD5D FF015130
DE724E5E D3F95392 E7BB16C4 A71D0F31B3A9926A 8F08EA00 FDC3A8F2 BB016DEC A3B9411B A2599A2A
8CB655C6 DFEA25BFEDDC73B5 94FAA0EF E595C612 A6AE5B8C 7F0CA19C EC4FE7AB 60546768
4BB2387D5F2F7EBD BC3EF0A6 04F6B404 01176925 02030100 01A381E9 3081E630 640603551D09045D 305B3010
06082B06 01050507 09043104 13024445 300F0608 2B06010505070903 31031301 46301D06 082B0601 05050709
01311118 0F313937 3131303134313230 3030305A 30170608 2B060105 05070902 310B0C09 4461726D
7374616474300E06 03551D0F 0101FF04 04030206 40301206 03551D20 040B3009 300706052B240801 01301F06
03551D23 04183016 80140001 02030405 06070809 0A0B0C0D0E0FFEDC BA983039 06082B06 01050507 0103042D
302B3029 06082B06 010505070B02301D 301B8119 6D756E69 63697061 6C697479 40646172 6D737461
64742E6465300D06 092A8648 86F70D01 01050500 03818100 8F8C80BB B2D86B75 F4E21F82EFE0F20F 6C558890
A6E73118 8359B9C7 8CE71C92 0C66C600 53FBC924 825090F295B08826 EAF3FF1F 5917C80B B4836129 CFE5563E
78592B5B B0F9ACB5 2915F0F2BC36991F 21436520 E9064761 D932D871 F71FFEBD AD648FA7 CF3C1BC0

96F112D4B882B39F E1A16A90 AE1A80B8 A9676518 B5AA7E97

C.4 Clé publique RSA de la CA

Ce paragraphe contient la clé publique RSA codée en DER de la CA qui a signé l'exemple de certificat. Elle est incluse pour simplifier les vérifications de l'exemple de certificat.

30818902818100c88f4bdb66f713ba3dd7a9069880e888d4321acb53cda7fcdfda89b834e25430b956d46a438baa6798035af30db
378424e00a8296b012b1b24f9cf0b3f83be116cd8a36957dc3f54cbd7c58a10c380b3dfa15bd2922ea8660f96e1603d81357c0442a
d607c5161d083d919fd5307c1c3fa6dfead0e6410999e8b8a8411d525dd0203010001

Références

Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2247] S. Kille et autres, "Utilisation des domaines dans les noms distinctifs LDAP/X.500", janvier 1998.

[RFC2616] R. Fielding et autres, "Protocole de transfert hypertexte -- HTTP/1.1", juin 1999. *(D.S., MàJ par* 2817, 6585)

[RFC2818] E. Rescorla, "HTTP sur TLS", mai 2000. *(Information)*

[RFC2985] M. Nystrom et B. Kaliski, "PKCS n° 9 : Classes d'objet et types d'attribut choisis, version 2.0", novembre 2000.

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

[X.509] Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, "Technologies de l'information - Interconnexion des systèmes ouverts – L'Annuaire : cadres de clé publique et de certificat d'attribut".

[X.520] Recommandation UIT-T X.520 (2001) | ISO/CEI 9594-6:2001, "Technologies de l'information - Interconnexion des systèmes ouverts – L'Annuaire : Types d'attribut choisis".

[X.680] Recommandation UIT-T X.680 (2002) | ISO/CEI 8824-1:2002), "Technologies de l'information - Notation n°1 de syntaxe abstraite".

[ISO 3166] ISO 3166-1:1997, "Codes pour la représentation des noms de pays", 1997.

Références pour information

[X.501] Recommandation UIT-T X.501 (2001) | ISO/CEI 9594-2:2001, "Technologies de l'information – Interconnexion des systèmes ouverts – L'Annuaire : Modèles".

[EU-ESDIR] Directive 1999/93/EC du Parlement Européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

[RFC2253] M. Wahl, S. Kille et T. Howes, "Protocole léger d'accès à un répertoire (LDAPv3) : Représentation de chaîne UTF-8 des noms distinctifs", décembre 1997.

Adresse des auteurs

Stefan Santesson
Microsoft Denmark
Tuborg Boulevard 12
DK-2900 Hellerup
Denmark
mél : stefans@microsoft.com

Tim Polk
NIST
Building 820, Room 426
Gaithersburg, MD 20899,
USA
mél : wpolk@nist.gov

Magnus Nystrom
RSA Security
Box 10704
S-121 29 Stockholm
Sweden
mél : magnus@rsasecurity.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement assuré par la Internet Society.