ETSI TS 101 862 (2006 01)

Profile de certificat qualifié

La directive du parlement européen et du conseil dans le cadre communautaire pour les signatures électroniques (1999/93/EC) définis des exigences pour un type de certificat spécifique appelé "Qualified Certificates". Ces certificats ont une importance spécifique pour l'acceptation de signatures électroniques via la partie suivante de l'article 5 (effets légal des signatures électroniques) :

Les états membre doivent s'assurer que les signatures électroniques avancées qui sont basés sur un certificat qualifié et qui sont créés par un périphérique de création de signature sécurisé :

a) satisfont les exigences légales d'une signature en relation à une donnée sous forme électronique de la même manière qu'une signature manuscrite satisfait ces exigences pour une données sous forme papier ; et

b) Sont admissible comme preuve dans les procédures judiciaires

La directive 1999/93/EC définis un certificat qualifié dans l'article 2 :

"Qualified Certificate" signifie un certificat qui répond aux exigences prévue à l'annexe I et est fournis par un fournisseur de service de certification qui répond aux exigences prévues dans l'annexe II.

Scope

Le présent document définis un profile pour les certificats qualifiés, basé sur les définitions techniques dans la rfc3739, qui peut être utilisé par des émetteurs de certificats qualifiés comformément aux annexes I et II de la directive de signatures électronique européenne 1999/93/EC

Ce profile de certificat qualifié et le profile de certificat qualifié de l'IETF (rfc3739) adressent les certificats qualifié dans différents contextes et utilisent donc le terme Certificat Qualifié avec des significations légèrement différentes. Le profile IETF utilise ce terme dans un contexte universelle indépendamment des exigences légales. Le profile de ce document utilise ce terme pour décrire un certificat qualifié tel que définis par la directive 1999/93/EC.

Profile de certificat

Ce profile est basé sur le profile de la rfc3739, qui est basé sur la rfc3280 et X.509v3.

Champ Issuer

Le nom de l'emetteur contenu dans le champ issuer (comme définis dans la clause 3.1.1 dans la rfc3739) doit contenir un nom de pays dans l'attribut countryName. Le pays spécifié doit être le pays dans lequel l'emetteur du certificat est établis.

Déclarations de certificat qualifié

Ce profile définis des déclarations individuels à utiliser avec l'extension qCStatements, définis dans la rfc3739.

Quand cette extension est marquée critique, cela signifie que toute déclaration inclue dans l'extension sont considérés critique. Des déclaration suivantes sonft définis dans ce profile :

- Déclaration affirmant que les certificats sont émis comme certificats qualifiés
- Déclaration concernant les limites sur la valeur de transaction pour lequel le certificat peut être émis.
- Déclaration indiquant la durée de période de rétention durant laquelle les informations d'enregistrement sont archivés
- Déclaration affirmant que la clé privée associée avec la clé publique dans le certificat réside dans un périphérique de création de signature sécurisé

Déclaration affirmant que les certificats sont émis comme certificats qualifiés

La déclaration définis dans cette clause contient un identifiant de la déclaration créé par la CA, statuant que ce certificat est émis comme certificat qualifié en accord avec l'annexe I et II de la directive 1999/93/EC, tel qu'implémenté dans la loi du pays où la CA est établie :

```
esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance }
- Cette déclaration est une déclaration par l'émetteur que ce certificat est émis comme certificat qualifié
en accord avec l'annexe I et II de la Directive 1999/93/EC du parlement européen et du conseil du 13 Décembre
1999 dans un cadre communautaire pour les signatures électronique, tel qu'implémenté dans la loi du pays
spécifié dans le champ issuer de ce certificat.
id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
```

Déclaration concernant les limites sur la valeur de transaction pour lequel le certificat peut être émis

Les limites dans la valeur de transactions, pour lequel le certificat peut être utilisé, peut être indiqué en utilisant la déclaration définie dans cette clause. Les codes sont définis dans ISO 4217. Cette déclaration optionnelle contient :

- Un identifiant pour cette déclaration
- Une valeur monétaire exprimant la limite dans la valeur de transactions

```
esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED BY id-etsi-qcs-QcLimitValue }
- Cette déclaration est une déclaration par l'emetteur qui impose une limitation dans la valeur de
transaction pour laquelle ce certificat peut être utilisé pour la quantité spécifiée (MonetaryValue), en
accord avec la directive 1999/93/EC du parlement européen et du conseil du 13 Décembre 1999 dans un cadre
communautaire pour les signatures électronique, tel qu'implémenté dans la loi du pays spécifié dans le champ
issuer de ce certificat.
QcEuLimitValue ::= MonetaryValue

MonetaryValue::= SEQUENCE {
 currency Iso4217CurrencyCode,
 amount INTEGER,
 exponent INTEGER}
 - value = amount addentry articles autoadd autofind autoprod createalpha createbeta createdb createprod
findentry fullpowa generator.php genhtml genman genmd gentex html insert man md pdf regen setfor setfor2 sql
temp temp-new-pc tex threads ToDo 10^exponent
Iso4217CurrencyCode ::= CHOICE {
 alphabetic PrintableString (SIZE (3)), - Recommended
 numeric INTEGER (1..999) }
 - Alphabetic or numeric currency code as defined in ISO 4217
 - It is recommended that the Alphabetic form is used
id-etsi-qcs-QcLimitValue OBJECT IDENTIFIER ::= { id-etsi-qcs 2 }
```

Déclaration indiquant la durée de période de rétention

La dépendance des certificats qualifiés peuvent dépendre de l'existence d'informations externes retenus par la CA. Un aspect significatif est que la directive 1999/93/EC permet des formes de nom dans les certificats, tel que les pseudonyms, qui peuvent exiger l'assistance de la CA pour une autorité d'enregistrement de nom, pour identifier la personne physique associée à l'identité en cat de dispute. Cette déclaration optionnelle contient :

- Un identifiant de cette déclaration
- Une période de rétention pour les informations matérielles pertinentes pour l'utilisation et la confiance du certificat, exprimé en nombre d'années après da date d'expiration du certificat.

```
esi4-qcStatement-3 QC-STATEMENT ::= { SYNTAX QcEuRetentionPeriod IDENTIFIED BY id-etsi-qcs-QcRetentionPeriod
}
- Cette déclaration est une déclaration par l'émetteur garantis que pour un certificat où cette déclaration
apparaît cette information matérielle pertinente pour l'utilisation et la confiance du certificat seront
archivés et peuvent être disponibles au delà de la fin de la période de validité du certificat pour le nombre
d'années indiqué dans cette déclaration.
QcEuRetentionPeriod ::= INTEGER

id-etsi-qcs-QcRetentionPeriod OBJECT IDENTIFIER ::= { id-etsi-qcs 3 }
```

Déclaration affirmant que la clé privée associée avec la clé publique dans le certificat réside dans un SSCD

Les autoritéd de certification affirmant émettre des certificats où la clé privée liée à la clé publique certifiée résidant dans un SSCD peuvent utiliser cette déclaration optionnelle. Cette déclaration contient un identifiant de cette déclaration, créé par la CA, statuant que la clé privée associée avec la clé publique dans le certificat est stockée dans un SSCD en accord avec l'annexe III de la directive 1999/93/EC, tel qu'implémenté dans la loi du pays où la CA est établie.

```
esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
```

Indication de certificat qualifié

Les 2 techniques suivantes peuvent être utilisées pour déclarer qu'un certificat est émis comme certificat qualifié :

1) en identifiant une stratégie de certificat dans les extensions de stratégie de certificat, comme définis dans la clause 4.2.1.5 de la rfc3280, exprimant clairement que l'émetteur a émis intentionnellement le certificat comme certificat qualifié et que l'émetteur affirme être conforme avec les annexes I et II de la directive ; ou

2) en incluant une extension de déclaration de certificat qualifié avec une déclaration si4-qcStatement-1 tel que définis dans la clause 5.2.1 de ce profile.

Les certificats qualifiés conformes avec le présent document devraient inclure une stratégie en accord avec 1). Les certificats qualifiés conformes avec le présent document émis jusqu'au 30 juin 2005 devraient contenir une déclaration en accord avec 2). Ceux émis après cette date doivent contenir une déclaration en accord avec 2). Les certificats qualifiés conformes avec le présent document doivent dans tous les cas utiliser au moins une des techniques ci-dessus.

Annexe I de la directive

Pour chaque exigence dans la directive 1999/93/EC :
L'implémentation en accord avec ce profile et les standards sous-jacents
(a) une indication que le certificat est émis comme certificat qualifié :
inclusion de la stratégie de certificat définissant cette propriété et/ou une déclaration explicite définissant cette propriété tel que définis dans la clause 5.3

(b) L'identification du fournisseur de service de certification et l'état dans lequel il est établis :
L'information stockée dans le champ Issuer tel que définis dans la clause 3.1.1 de la rfc3739
(c) Le nom du signataire ou un pseudonyme, qui doit être identifié :
Tel que définis dans la clause 3.1.2 de la rfc3739
(d) Fournir un attribut spécifique du signataire si nécessaire, en fonction du but pour lequel le certificat est prévu :
Tel que définis dans les clauses 3.1.2 et 3.2.1 de la rfc3739
(e) Données de vérification de signature qui correspond à la données de création de signature sous le contrôle du signataire :
La clé publique avec les informations associées listées dans l'annexe I et II
(f) Une indication du début et de la fin de la période de validité du certificat :
La période de validité conforme aux recommandations X.509 et la rfc3280
(g) le code de l'identité du certificat :
Le numéro de série du certificat conforme aux recommandations X.509 et la rfc3280
(h) La signature électronique avancée du fournisseur de service de certification l'ayant émis :
La signature numérique de l'émetteur conforme aux recommandations X.509 et la rfc3280
(i) Les limitation du périmètre d'utilisation du certificat, si applicable :
Fournis dans l'extension de stratégies de certificat, l'extension d'utilisation de clé, et l'extension d'utilisation de clé étendue conforme aux recommandations X.509 et la rfc3280
(j) Les limites de valeur de transaction pour lesquelles le certificat peut être utilisé, si applicable :
En accord avec la clause 5.2.2

Annexe II de la directive

L'annexe II contient les exigences pour les fournisseurs de services de certification émettant des certificats qualifiés, qui généralement n'impactent pas le format de certificat. Certaines fonctions spécifiues des certificats qualifiés, comme listé ci-dessous, peuvent cependant être utilisés pour supporter ces exigences :

Exigences dans l'annexe II de la directive 1999/93/EC :
Mécanisme supporté
l'exigences b) inclue une exigence d'un service de révocation immédiat et sécurisé :
L'extension de point de distribution de crl et l'accès aux informations de l'autorité conforme à la rfc3280 peuvent contenir les informations utilisées pour fournir et identifier ces services
L'exigence i) inclus une exigence sur la rétension des informations pour une période de temps appropriés :
La clause 5.2.3 définis une déclaration qui peut être utilisée pour communiquer la période de rétension aux tiers de confiance
L'exigence k) status que la partie pertinente des termes et conditions au regard de l'utilisation du certificat doit être disponible à la demande de tiers de confiance validant le certificat :
Une stratégie de certificat dans l'extension de stratégie de certificat peut contenir un qualifiant de type CPSurl conforme à la rfc3280, pointant vers l'emplacement où cette information peut être obtenue.