Sommaire

1. Résumé et domaine d'application 2
2. Responsabilités 2
3. Profil des certificats émis par les AC du Notariat 3
3.1 Format général du Certificat X.509 des NOTAIRES 4
3.1.1 Informations de base 4
3.2 Extensions standard utilisées dans le certificat X.509 Notaires 4
3.2.1 Authority Key Identifier 4
3.2.2 Subject Key Identifier 4
3.2.3 KeyUsage (extension toujours marquée critique) 4
3.2.4 CertificatePolicies 4
3.2.5 BasicConstraints 4
3.2.6 Subject Alt Name 4
3.2.7 Qualified Certificate Statements (1.3.6.1.5.5.7.1.3) 5
3.3 Description des certificats 6
3.3.1 Les certificats du Niveau Racine (CA ROOT) 6
3.3.2 Les certificats du Niveau Autorité de Certification (CA) 7
3.3.3 Les certificats du Niveau Utilisateur émis par l'AC REAL 8
3.3.4 Les certificats du Niveau Opérateur ou Serveur émis par l'AC REALTECH 11
3.3.5 Les certificats de signature des réponses OCSP 16
3.3.6 Les certificats de services applicatifs émis par l'AC REALTS 17
3.4 Description des OID de politiques 19
3.4.1 Prise en compte des différents environnements 19
3.4.2 AC Professions Réglementées 19
3.4.3 AC Notaires 19
3.4.4 AC REAL 19
3.4.5 AC REALTECH 20
3.4.6 AC REALTS 20
3.4.7 Un titulaire notaire signé par REAL 20
3.4.8 Un titulaire collaborateur signé par REAL 23
3.4.9 Les certificats signés par l'AC REALTECH 24
3.4.10 Les certificats signés par l'AC REALTS 25

4. Profil d'une LCR 26
4.1 Champs et extensions des CRL 27
5. Profil d'une réponse OCSP 27
6. Les points de contrôle 28
7. Documents attachés 28

1. Résumé et domaine d'application

Cette procédure décrit le format des certificats et des CRL émis par la PKI du Notariat.

2. Responsabilités

Ce document est sous la responsabilité du responsable de l'OSC.

3. Profil des certificats émis par les AC du Notariat

Certificat

Contenu du certificat

Version		
Numéro de série		
Information sur la signature du certificat par l'AC (algorithmes et paramètres)		
Nom du fournisseur du certificat		
Période de validité du certificat		
Nom du porteur de certificat		
Information sur la clé publique (valeur de la clé publique, algorithme et paramètre)		
Nom unique du fournisseur du certificat		
Nom unique du porteur du certificat		
Identifiant du type de l'extension	Criticité (oui/non)	Valeur
Identifiant du type de l'extension	Criticité (oui/non)	Valeur
Identifiant du type de l'extension	Criticité (oui/non)	Valeur
.....		

Algorithme de signature du certificat par l'AC

Algorithme
Paramètres

Signature numérique du certificat

Valeur de la signature numérique par l'AC

3.1 Format général du Certificat X.509 des NOTAIRES

3.1.1 Informations de base

Les informations de base du certificat sont:

- Numéro de série
- Nom du fournisseur du certificat
- Période de validité du certificat
- Nom du porteur de certificat

3.2 Extensions standard utilisées dans le certificat X.509 Notaires

3.2.1 Authority Key Identifier

Cette extension identifie la clé publique à utiliser (empreinte) pour vérifier la signature d'un certificat.

3.2.2 Subject Key Identifier

Cette extension identifie la clé publique du certificat. Elle est nécessaire pour utiliser les AKI.

3.2.3 KeyUsage (extension toujours marquée critique).

Cette extension définit l'utilisation prévue de la clé publique certifiée :

digitalSignature	(0),	(clé d'authentification)
nonRepudiation	(1),	(clé de signature)
keyEncipherment	(2),	(clé de confidentialité)
keyCertSign	(5),	(clé de signature de certificats)
cRLSign	(6),	(clé de signature de CRLs)

Cette extension est critique.

3.2.4 CertificatePolicies

Cette extension définit les politiques de certification que le certificat reconnaît supporter. Voir le

document « Plan d'attribution des OID de Politiques de Certification ».

3.2.5 BasicConstraints

Cette extension indique si un titulaire peut agir comme une autorité de Certification (CA) en utilisant sa clé privée pour signer les certificats.

Cette extension est présente et critique uniquement pour les autorités de certification.

3.2.6 Subject Alt Name

Cette extension indique l'adresse email. Uniquement pour les titulaires.

3.2.7 Qualified Certificate Statements (1.3.6.1.5.5.7.1.3)

Cette extension indique que le certificat est qualifié (uniquement pour les certificats de signature émis par l'AC REAL).

Les extensions suivantes ont été également positionnées en dessous de cet OID:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) : Indique que le certificat est qualifié
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4): Indique que le la bi-clé associée au certificat a été générée par un SSCD.

3.3 Description des certificats

3.3.1 Les certificats du Niveau Racine (CA ROOT)

Certificat de la Clé de certification (self signed).
NB: Ce certificat sert aussi à la signature des ARL

Objet	Format	Certificat de clé de certification CA ROOT
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	C=FR, o=Professions Réglementées Ou C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, OU = ProfessionsReglementees2028
Validity	UTCTime	Not before <<date création>> NotAfter : date création + 16 ans
Subject	PrintString	C=FR, o=Professions Réglementées Ou C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, OU = ProfessionsReglementees2028
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP CA ROOT Ou Clé publique 512 octets + exposant publique =65537 = KP CA ROOT
Extensions	Seq	
AuthorityKey ID	OctString	N.U
Key Usage	Seq	
Critical	Boolean	True
Value	Bitstring	Key cert Sign , value (bit 5), CRLSign (bit6)
Authority Key identifier	Seq	Yes
Critical	Boolean	No
Subject Key identifier		Uniquement pour les certificats croisés
BasicConstraint		
Critical	Boolean	True
SubjectAltName	IA5string	N.U
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée de CA ROOT (256 octets)

3.3.2 Les certificats du Niveau Autorité de Certification (CA)

Certificat de la Clé de certification signé par le CA ROOT.
NB: Ce certificat sert aussi à la signature des CRL

Pour l'AC Notaires2023 et les AC issues de cette dernière, le DN du certificat est constitué ainsi :

C=FR	O = CONSEIL SUPERIEUR DU NOTARIAT	OU = 0002 784350134	**CN = XXX**

Avec XXX = nom de l'AC.

Pour l'ensemble des autres AC :

C=FR	O = CONSEIL SUPERIEUR DU NOTARIAT	OU = 0002 784350134	**OU = XXX**

Avec XXX = nom de l'AC.

Objet	**Format**	**Certificat de clé de certification CA**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation' ou Numéro de série aléatoire préfixé du condensat du DN de l'AC (pour les certificats d'AC issus de Notaires2023)
Signature	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter : date création + 4 ans ou 8 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP CA
Extensions	Seq	
AuthorityKey ID	OctString	N.U
Key Usage	Seq	
Critical	Boolean	True
Value	Bitstring	Key cert Sign , value (bit 5), CRLSign (bit6)
Authority Key identifier	Seq	Yes
Critical	Boolean	No
Subject Key identifier		Yes
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
BasicConstraint		
Critical	Boolean	True
SubjectAltName	IA5string	N.U
SignatureAlgorithm	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée de CA ROOT (256 octets)

* Valeur de l'extension CRL Distribution Point :
Pour les certificats de l'autorité « Notaires » la valeur est :
http://www.preuve-electronique.org/ListeRevocations/professionsreglementees.arl ou
http://www.preuve-electronique.org/ListeRevocations/professionsreglementees2028.arl

Pour les certificats des autorités « REAL », « REALTS » et « REALTECH » la valeur est :
http://www.preuve-electronique.org/ListeRevocations/notaires.arl
ou
http://www.preuve-electronique.org/ListeRevocations/notaires2018.arl ou
http://www.preuve-electronique.org/ListeRevocations/notaires2020.arl ou
http://www.preuve-electronique.org/ListeRevocations/notaires2023.arl

** Valeur de l'extension CertificatePolicies :
- OID du certificat
- contient également l'oid et l'url de la PC de l'AC

3.3.3 Les certificats du Niveau Utilisateur émis par l'AC REAL Les

certificats de niveau utilisateur sont les suivants :
- Certificat de la clé de signature.
- Certificat de la clé d'authentification.
- Certificat de la clé de confidentialité

1- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=Professions Réglementées	OU = Notaires	OU = AC déléguée	OU = REAL	**CN**

2- Le **CN** du sujet de chacun de ces certificats est formaté ainsi : Nom Prénom (**n° de titulaire**) 3- Le

N° de titulaire est un numéro à 10 chiffres formaté ainsi :

3	Code CRPCEN de l'office du titulaire	**0**	Profil du titulaire : • 1 Chiffre pair : Notaire • 1 Chiffre impair : Collaborateur	Compteur de 00 à 99

Objet	**Format**	**Certificat de clé de signature**	**Certificat clé d'authentification**
Certificate	Seq		
TBSCertificate	Seq		
Version	Integer	2 (version 3)	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString		
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans	Not before <<date création>> NotAfter = date création + 2 ans

Objet	Format	Certificat de clé de signature	Certificat clé d'authentification
Subject	PrintString		
SubjectPublicKeyInfo	Seq		
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*	Yes*
Certificatepolicie		Yes**	Yes**
Extensions	Seq		
AuthorityKey ID	OctString	Yes	Yes
Key Usage	Seq		
Critical	Boolean	TRUE	TRUE
Value	Bitstring	Non repudiation , value (bit 1)	Digital signature , value (bit 0)
BasicConstraint			
Critical	Boolean	N.U	N.U
Authority Key identifier		Yes	Yes
SubjectAltName	IA5string	Email du porteur	Email du porteur
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)	Signature calculée avec la clé privée du CA (256 octets)
Qualified certificate statements : 1.3.6.1.5.5.7.1.3	Seq	Yes	No
Utilisation avancée de la clé	Seq	N.U	Authentification du client (1.3.6.1.5.5.7.3.2) Ouverture de session par carte à puce (1.3.6.1.4.1.311.20.2.2)

Objet	Format	Certificat de clé de confidentialité
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	

Objet	Format	Certificat de clé de confidentialité
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	N.U
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Key Encipherment , value (bit 2)
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du porteur
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)
Qualified certificate statements : 1.3.6.1.5.5.7.1.3	Seq	No
Utilisation avancée de la clé	Seq	N.U

* Valeur de l'extension CRL Distribution Point :
http://www.preuve-electronique.org/ListeRevocations/real.crl ou
http://www.preuve-electronique.org/ListeRevocations/real2014.crl ou
http://www.preuve-electronique.org/ListeRevocations/real2016.crl ou
http://www.preuve-electronique.org/ListeRevocations/real2017.crl ou
http://www.preuve-electronique.org/ListeRevocations/real2019.crl

** Valeur de l'extension CertificatePolicie :

- L'OID du certificat
- L'OID et l'URL de la PC de l'AC REAL correspondante

3.3.4 Les certificats du Niveau Opérateur ou Serveur émis par l'AC REALTECH

Les certificats émis par l'AC REALTECH sont les suivants :

- Certificat de la clé d'authentification pour les opérateurs ;
- Certificat de la clé d'authentification pour les serveurs SSL ;
- Certificat de la clé de signature pour les serveurs de signature ;
- Certificat de la clé de signature pour les serveurs d'horodatage RGS V1;

3.3.4.1 Certificat de la clé d'authentification pour les opérateurs

1- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=REAL.NOT	OU = 0002 **509242988**	**CN**

2- Le **CN** du sujet de chacun de ces certificats est formaté ainsi :

Prénom NOM	**OPERATEUR**	*Facultatif : (39999701xx) avec xx compris entre 00 et 99*

Objet	**Format**	**Certificat clé d'authentification**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Digital signature, value (bit 0)
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du porteur
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)
Utilisation avancée de la clé	Seq	Authentification du client (1.3.6.1.5.5.7.3.2)

* Valeur de l'extension CRL Distribution Point : http://www.preuve-electronique.org/ListeRevocations/realtech.crl ou http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl

ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl ou
http://www.preuve-electronique.org/ListeRevocations/realtech2019.crl

** Valeur de l'extension CertificatePolicie :

- L'OID du certificat
- L'OID et l'URL de la PC REALTECH

3.3.4.2 Certificat de la clé d'authentification pour les Serveurs SSL

1- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=**Entité**	OU = 0002 **N° de SIREN**	**CN**

2- **Entité** : nom de l'entité (exemple : REAL.NOT)
3- **N° de SIREN** (exemple : **509242988** pour REAL.NOT)
4- Le **CN** du sujet de chacun de ces certificats contient le FQDN du serveur.

Objet	**Format**	**Certificat clé d'authentification**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Cryptage de clé (40)
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du contact
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)
Utilisation avancée de la clé	Seq	Authentification du serveur (1.3.6.1.5.5.7.3.1)

* Valeur de l'extension CRL Distribution Point : http://www.preuve-electronique.org/ListeRevocations/realtech.crl ou

http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl ou
http://www.preuve-electronique.org/ListeRevocations/realtech2019.crl

** Valeur de l'extension CertificatePolicie ;

- L'OID du certificat
- L'OID et l'URL de la PC REALTECH

3.3.4.3 Certificat de la clé de signature pour les Serveurs de signature

1- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=REAL .NOT	OU = 0002 509242988	**CN**

2- Le **CN** du sujet de chacun de ces certificats est formaté ainsi :

Serveur de signature	Compteur : 00 à 99

Objet	**Format**	**Certificat clé d'authentification**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) ou Sha-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Digital Signature
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du contact
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)
Utilisation avancée de la clé	Seq	

* Valeur de l'extension CRL Distribution Point :

http://www.preuve-electronique.org/ListeRevocations/realtech.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2019.crl

** Valeur de l'extension CertificatePolicie :

- L'OID du certificat
- L'OID et l'URL de la PC REALTECH

3.3.4.4 Certificat de la clé de signature pour les Serveurs d'horodatage RGS V1

1- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=CONSEIL SUPERIEUR DU NOTARIAT	OU = 0002 784350134	OU = AH Notaires	**CN**

2- Le **CN** du sujet de chacun de ces certificats est formaté ainsi :

UH Notaires	X	date de génération du certificat au format aaaammjjhhmmss

Avec x = n° d'incrément en PROD et PP en Pré Production

Objet	**Format**	**Certificat clé d'authentification**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Digital Signature
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du contact
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)

* Valeur de l'extension CRL Distribution Point :

http://www.preuve-electronique.org/ListeRevocations/realtech.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl

Utilisation avancée de la clé	Seq	PKIX key purpose timeStamping (1.3.6.1.5.5.7.3.8)

* Valeur de l'extension CRL Distribution Point :

http://www.preuve-electronique.org/ListeRevocations/realtech.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl

** Valeur de l'extension CertificatePolicie :
- L'OID du certificat
- L'OID et l'URL de la PC REALTECH

3.3.4.5 Certificat multi-usage pour serveur MICEN

3- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=REAL.NOT	OU = 0002 509242988	**CN**

4- Le **CN** du sujet de chacun de ces certificats est formaté ainsi :

SERVEUR MICEN	x

Avec x = n° d'incrément en PROD et PP en Pré Production

Objet	**Format**	**Certificat clé d'authentification**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation'
Signature	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Digital Signature, Key encipherment, non repudiation
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du contact
SignatureAlgorithm	OID	Sha-1 avec RSA encryption (1.2.840.113549.1.1.5) Ou SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)
Utilisation avancée de la clé	Seq	N/A

* Valeur de l'extension CRL Distribution Point : http://www.preuve-

http://www.preuve-electronique.org/ListeRevocations/realtech.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl
ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl
electronique.org/ListeRevocations/realtech.crl

ou
http://www.preuve-electronique.org/ListeRevocations/realtech2016.crl ou
http://www.preuve-electronique.org/ListeRevocations/realtech2017b.crl ou
http://www.preuve-electronique.org/ListeRevocations/realtech2019.crl

** Valeur de l'extension CertificatePolicie :

- L'OID du certificat
- L'OID et l'URL de la PC REALTECH

3.3.5 Les certificats de signature des réponses OCSP.

Un certificat est émis pour chacune des AC suivante et signe les réponses OCSP :

- Notaires
- REAL
- REALTECH
- REALTS

5- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=Professions Réglementées	OU = Notaires	**CN**

6- Le **CN** du sujet de chacun de ces certificats est formaté ainsi :

REPONDEUR OCSP	x

Avec x = identifiant de l'AC-x, x n° chronologique

Objet	Format	Certificat clé d'authentification
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	"créé à l'initialisation' ou numéro de série aléatoire préfixé du condensat du DN de l'AC
Signature	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Digital signature, value (bit 0)
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du porteur
SignatureAlgorithm	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)

Utilisation avancée de la clé	Seq	Signature OCSP (1.3.6.1.5.5.7.3.9)

3.3.6 Les certificats de services applicatifs émis par l'AC REALTS

Les certificats émis par l'AC REALTS sont les suivants :

- Certificat de la clé de signature pour les serveurs d'horodatage RGS V2;
- Certificat de la clé de signature pour les serveurs d'horodatage eIDAS
- Certificat de signatures des jetons OCSP associés

3.3.6.1 Certificat de la clé de signature pour les Serveurs d'horodatage RGS V2/eIDAS

7- Le DN de chacun de ces certificats est formaté ainsi :

C=FR	O=CONSEIL SUPERIEUR DU NOTARIAT	OU = 0002 784350134	OU = AH Notaires	**CN**

8- Le **CN** du sujet de chacun de ces certificats est formaté ainsi :

REAL.SES.UH.	X	.date de génération du certificat au format aaaammjjhhmmss

Avec x = n° d'incrément en PROD et PP en Pré Production

Ou

REAL.not.SES.UH.	X	.date de génération du certificat au format aaaammjjhhmmss

Avec x = n° d'incrément en PROD et PP en Pré Production

Objet	**Format**	**Certificat clé d'authentification**
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire préfixé du condensat du DN de l'AC
Signature	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
Issuer	PrintString	
Validity	UTCTime	Not before <<date création>> NotAfter = date création + 2 ans
Subject	PrintString	
SubjectPublicKeyInfo	Seq	
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Clé publique 256 octets +exposant publique =65537 = KP Client
CrlDistributionPoint		Yes*
Certificatepolicie		Yes**
Extensions	Seq	
AuthorityKey ID	OctString	Yes
Key Usage	Seq	
Critical	Boolean	TRUE
Value	Bitstring	Digital Signature
BasicConstraint		
Critical	Boolean	N.U
Authority Key identifier		Yes
SubjectAltName	IA5string	Email du contact
SignatureAlgorithm	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11)
SignatureValue	BitString	Signature calculée avec la clé privée du CA (256 octets)
Utilisation avancée de la clé	Seq	PKIX key purpose timeStamping (1.3.6.1.5.5.7.3.8)

* Valeur de l'extension CRL Distribution Point :
http://www.preuve-electronique.org/ListeRevocations/realts2019.crl

** Valeur de l'extension CertificatePolicie :

- L'OID du certificat
- L'OID et l'URL de la PC REALTS

3.4 Description des OID de politiques

Les chapitres ci-dessous décrivent les valeurs à mettre dans l'extension CertificatePolicies

3.4.1 Prise en compte des différents environnements

Afin de prendre en compte des différents environnements (production, pré production, pré validation …), une distinction dans les OID permet de cloisonner les certificats dans chaque environnement. Pour ce faire, on s'appuie sur le document [REF01].

On notera dans la suite du document ***1.2.250.1.78.*1.X** comme étant la racine pour une autorité avec :
X = 1 pour « Professions réglementées » dans l'environnement de production,
X = 2 pour « Professions réglementées » dans l'environnement de pré production,
X = 3 pour « Professions réglementées » dans l'environnement d'évaluation,
X = 4 pour « Professions réglementées » dans l'environnement de l'environnement de test (CSN).

3.4.2 AC Professions Réglementées

Le certificat de 2048 bits est autosigné. OID du certificat de signature de certificats :

Politique de certification Professions Réglementées	1.2.250.1.78	.1	.X	**.1.1**

Le certificat de 4096 bits est autosiqné. OID du certificat de signature de certificats :

Politique de certification Professions Réglementées	1.2.250.1.78	.1	.X	**.1.3**

+

Notaires_Classe4_OR_SignatureAC				Classe		cat.	use
	1.2.250.1.78	.1	.X	**.2**	**.4**	**.3**	**.4**

3.4.3 AC Notaires

Le certificat de 2048 bits est signé par Professions Réglementées. OID du certificat de signature de certificats :

Politique de certification Professions Réglementées	1.2.250.1.78	.1	.X	**.1.1**
	ou			
	1.2.250.1.78	.1	.X	**.1.3**

+

Notaires_Classe4_OR_SignatureAC					Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	**.2**	**.4**	**.3**	**.4**

3.4.4 AC REAL

Le certificat de 2048 bits est signé par Notaires. OID du certificat de signature de certificats :

Politique de certification de Notaires	1.2.250.1.78	.1	.X	.3.1.	**.1.1**
	Ou				
	1.2.250.1.78	.1	.X	.3.1.	**.1.3**

	Ou 1.2.250.1.78 .1 .X .3.1. **.1.5**
+	
REAL_Classe4_OR_SignatureAC	1.2.250.1.78 .1 .X .3.1. .3.1 — Classe: **.2** **.4** — cat.: **.3** — use: **.4**

3.4.5 AC REALTECH

Le certificat de 2048 bits est signé par Notaires. OID du certificat de signature de certificats :

Politique de certification de Notaires	1.2.250.1.78 .1 .X .3.1. **.1.1** Ou **.1.3** Ou 1.2.250.1.78 .1 .X .3.1. **.1.5**
+	
REALTECH_Classe4_OR_SignatureAC	1.2.250.1.78 .1 .X .3.1. .3.4 — Classe: **.2** **.4** — cat.: **.3** — use: **.4**

3.4.6 AC REALTS

Le certificat de 2048 bits est signé par Notaires. OID du certificat de signature de certificats :

Politique de certification de Notaires	1.2.250.1.78 .1 .X .3.1. **.1.5**
+	
REALTS_Classe4_OR_SignatureAC	1.2.250.1.78 .1 .X .3.1. .3.5 — Classe: **.2** **.4** — cat.: **.3** — use: **.4**

3.4.7 Un titulaire notaire signé par REAL

3.4.7.1 Dans l'environnement PSCE avec qualification

Le certificat de 2048 bits est signé par REAL (avec qualification PSCE). La politique de certification est composée de :

- **Pour la signature**

Politique de certification de REAL qualifiée PSCE	1.2.250.1.78 .1 .X .3.1. .3.1 **.1.8** **ou** **.1.10** **ou** **.1.12** **ou** 1.2.250.1.78 .1 .X .3.1. .3.1 **.1.14**

	ou 1.2.250.1.78 .1 .X .3.1 .3.1 **.1.17** ou 1.2.250.1.78 .1 .X .3.1 .3.1 **.1.20** ou 1.2.250.1.78 .1 .X .3.1. .3.1 **.1.22**
REAL_Classe2_OR_Signature	Classe cat. use 1.2.250.1.78 .1 .X .3.1. .3.1 **.2** **.2** **.3** **.1**

- **Pour la signature d'actes authentique**

Politique de certification de REAL qualifiée PSCE	1.2.250.1.78 .1 .X .3.1. .3.1 **.1.8** ou **.1.10** ou **.1.12** ou **.1.14** ou 1.2.250.1.78 .1 .X .3.1. .3.1 **.1.17** 1.2.250.1.78 .1 .X .3.1. .3.1 **.1.20** 1.2.250.1.78 .1 .X .3.1. .3.1 **.1.22**
REAL_Classe2_PLATINE_Signature	Classe cat. use 1.2.250.1.78 .1 .X .3.1. .3.1 **.2** **.2** **.4** **.1**

- **Pour l'authentification**

Politique de certification de REAL authentification	1.2.250.1.78 .1 .X .3.1. .3.1 **.1.3**
REAL_Classe2_OR_Authentification	Classe cat. use 1.2.250.1.78 .1 .X .3.1. .3.1 **.2** **.2** **.3** **.2**

- **Pour le chiffrement**

Politique de certification de REAL chiffrement	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.4**				
REAL_Classe2_OR_Chiffrement						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.3**	

3.4.7.2 Dans l'environnement PSCE avant la qualification

Le certificat de 2048 bits est signé par REAL (dans l'environnement PSCE). La politique de certification est composée de :

- **Pour la signature**

Politique de certification de REAL déposé PSCE	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.2**				
REAL_Classe2_OR_Signature						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.1**	

- **Pour la signature d'actes authentique**

Politique de certification de REAL déposé PSCE	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.2**				
REAL_Classe2_PLATINE_Signature						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.4**	**.1**	

- **Pour l'authentification**

Politique de certification de REAL authentification	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.3**				
REAL_Classe2_OR_Authentification						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.2**	

- **Pour le chiffrement**

Politique de certification de REAL chiffrement	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.4**				
REAL_Classe2_OR_Chiffrement						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.3**	

3.4.7.3 Avant l'environnement PSCE

Le certificat de 1024 bits est signé par REAL. La politique de certification est composée de :

Politique de certification de REAL	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.1**

+ l'un des trois :

REAL_Classe2_OR_Signature						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.1**	
REAL_Classe2_OR_Authentification						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.2**	
REAL_Classe2_OR_Chiffrement						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.2**	**.3**	**.3**	

3.4.8 Un titulaire collaborateur signé par REAL

3.4.8.1 Dans l'environnement PSCE avec qualification

Le certificat de 2048 bits est signé par REAL avec la conformité PSCE. La

politique de certification est composée de :

Pour la signature :

Politique de certification de REAL qualifiée PSCE	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.8**				
	ou									
						.1.10				
	ou									
						.1.12				
	ou									
						.1.14				
	ou									
	1.2.250.1.78	.1	.X	.3.1	.3.1	**.1.17**				
	Ou									
	1.2.250.1.78	.1	.X	.3.1	.3.1	**.1.20**				
	ou									
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.22**				
REAL_Classe1_OR_Signature						Classe		cat.	use	
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.1**	

Pour l'authentification:

Politique de certification de REAL authentification	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.3**			
REAL_Classe1_OR_Authentification						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.2**

Pour le chiffrement :

Politique de certification de REAL chiffrement	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.4**			
REAL_Classe1_OR_Chiffrement						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.3**

3.4.8.2 Dans l'environnement PSCE avant la qualification

Le certificat de 2048 bits est signé par REAL avec la conformité PSCE. La politique de certification est composée de :

Pour la signature :

Politique de certification de REAL déposé PSCE	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.2**			
REAL_Classe1_OR_Signature						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.1**

Pour l'authentification:

Politique de certification de REAL authentification	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.3**			
REAL_Classe1_OR_Authentification						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.2**

Pour le chiffrement :

Politique de certification de REAL chiffrement	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.4**			
REAL_Classe1_OR_Chiffrement						Classe		cat.	use

	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.3**

3.4.8.3 Avant la conformité PSCE

Le certificat de 1024 bits est signé par REAL. La politique de certification est composée de

Politique de certification de REAL	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.1.1**	

+ l'un des trois :

REAL_Classe1_OR_Signature						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.1**
REAL_Classe1_OR_Authentification						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.2**
REAL_Classe1_OR_Chiffrement						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.1	**.2**	**.1**	**.3**	**.3**

3.4.9 Les certificats signés par l'AC REALTECH

3.4.9.1 Les certificats d'authentification pour les opérateurs

Le certificat de 2048 bits est signé par REALTECH. La politique de certification est composée de

Politique de certification REALTECH	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.1**	
	ou						
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.5**	

+

						service	Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.4.Y**	**.2**	**.5**	**.2**	**.1**

3.4.9.2 Les certificats d'authentification pour les serveurs SSL

Le certificat de 2048 bits est signé par REALTECH. La politique de certification est composée de

Politique de certification REALTECH	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.1**	
	ou						
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.5**	

+

						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.2**	**.0**	**.2**	**.3**

3.4.9.3 Les certificats de signature pour serveur de signature

Le certificat de 2048 bits est signé par REALTECH. La politique de certification est composée de

Politique de certification REALTECH	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.1**	
	ou						
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.5**	

+

						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.2**	**.0**	**.3**	**.1**

3.4.9.4 Les certificats de signature pour serveur d'horodatage

Le certificat de 2048 bits est signé par REALTECH. La politique de certification est composée de

Politique de certification REALTECH	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.1**
	ou					
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.3**

+

						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.2**	**.0**	**.3**	**.1**

3.4.9.5 Les certificats multi-usagepour serveur MICEN

Le certificat de 2048 bits est signé par REALTECH. La politique de certification est composée de

Politique de certification REALTECH	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.1**
	ou					
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.1.5**

+

						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.4	**.2**	**.0**	**.3**	**.7**

3.4.10 Les certificats signés par l'AC REALTS

3.4.10.1 Les certificats de signature pour serveur d'horodatage Le certificat de 2048 bits est signé par REALTS. La politique de certification est composée de

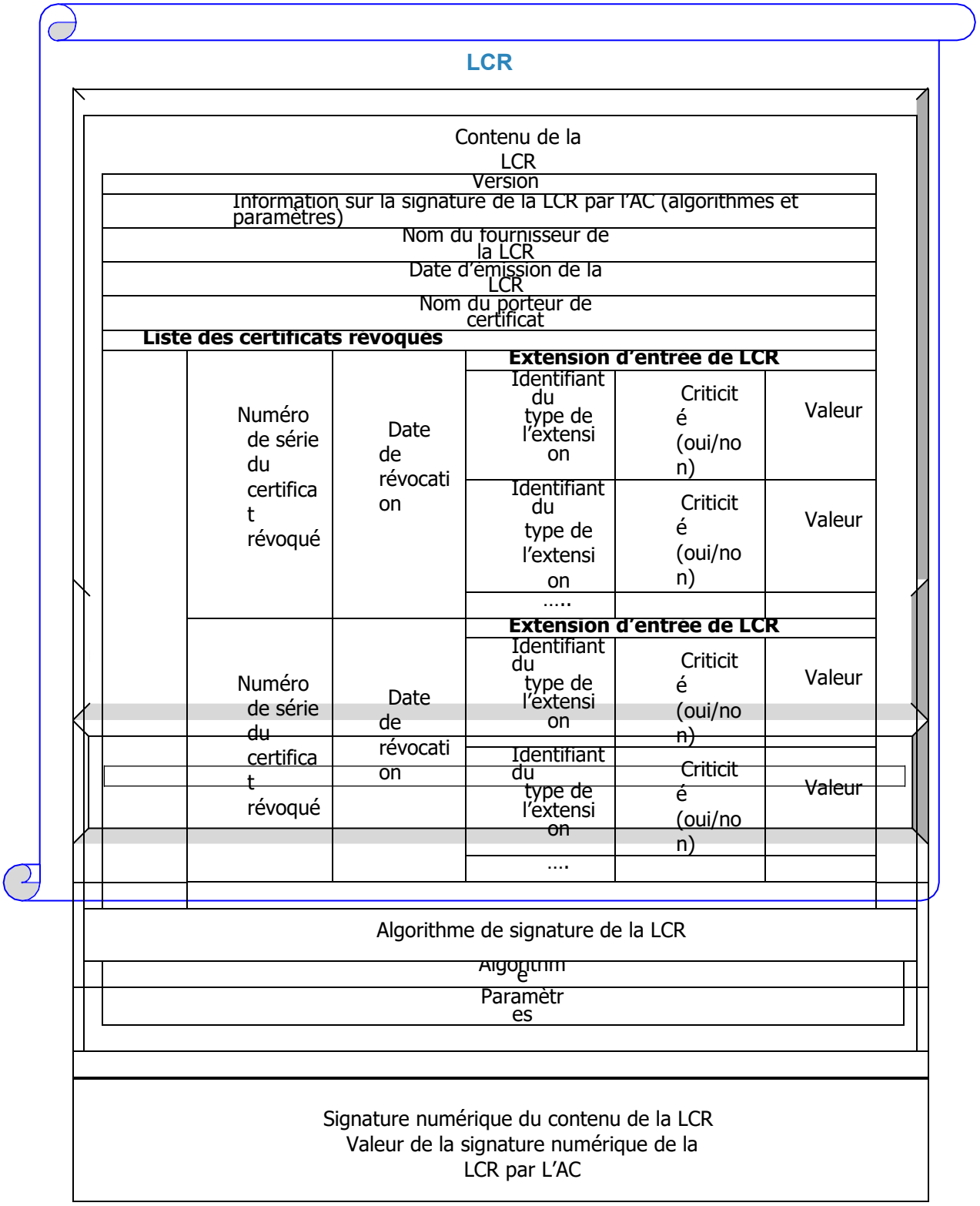
Politique de certification REALTS	1.2.250.1.78	.1	.X	.3.1.	.3.5	**.1.1**

+

						Classe		cat.	use
	1.2.250.1.78	.1	.X	.3.1.	.3.5	**.2**	**.0**	**.3**	**.1**

4. Profil d'une LCR

Toutes les listes de révocations de certificats émis par les AC du Notariat ont le même format.



4.1 Champs et extensions des CRL

La PKI produit pour chaque AC, une CRL toutes les 12h avec une durée de vie de 24h.

Champ	Valeur
Version	V2
Signature	Le champ signatureAlgorithm contient l'identifiant de l'algorithme de signature de la CRL
Issuer	L'émetteur du signataire de la liste de révocation a comme DN: Ce niveau peut révoquer les certificats immédiatement inférieur, entre autre ceux de l'autorité de certification CA. Soit au niveau supérieur : Niveau Autorité Root Soit au niveau inférieur : Niveau Autorité
This Update	Ce champs défini la date et l'heure de l'émission de CETTE CRL. Le format UTC Time est utilisé pour ce champ.
Next Update	Ce champs défini la prochaine date et heure de l'émission programmée de la prochaine CRL. Le format UTC Time est utilisé pour ce champ.
Certificats révoqués	Les certificats révoqués sont listés. Les certificats sont référencés par leur n° de série. La date de révocation est précisée pour chacun des certificats listés. La raison de révocation n'est pas renseignée, sauf pour l'AC REALTS.
CRL Number	N° de la CRL
Authority Key Identifier	Cette extension identifie la clé publique à utiliser (empreinte) pour vérifier la signature d'une CRL.

5. Profil d'une réponse OCSP

Une réponse correspond à un certificat.

Les réponses OCSP des AC REAL, REALTECH, REALTS et NOTAIRES sont composées ainsi :

Champ	Valeur
Version	1
ResponseId	DN du certificat de signature de la réponse OCSP
ProducedAt	Date de production de la réponse (GMT)
Responses	
Certificate ID	
Hash Algorithm	Sha256
Issuer Name	Hash du DN du certificat vérifié
Issuer Key hash	Hash de la clé publique du certificat vérifié
Serial Number	N° de série du certificat vérifié
Cert Status	Statut du certificat : revoked / good
Revocation time	*Si le certificat est révoqué : Date de révocation (GMT)*
Revocation reason	*Si le certificat est révoqué : Raison de la révocation*
This update	Identique à la date de production de la réponse
Signature de la réponse	Signature Sha256WithRSAEncryption
Certificate	Certificat vérifié

6. Les points de contrôle

- Vérifier les gabarits des certificats émis par les différentes AC.

7. Documents attachés

- *Plan d'attribution des OID*