Description des certificats et CRL de la chaîne d'AC Notaires de France

DESCRIPTION DES CERTIFICATS ET CRL DE LA CHAINE D'AC NOTAIRES DE FRANCE

Historique des modifications :

Version	Date	Rédacteur (s)	Modification(s) apportée(s)
5.0	16/11/2020	ADSN	• Modification du DN des certificats d'horodatage : remplacement de REAL.NOT.SES.UH par ADSN.SDC.UH.Ajout d'un sommaire • Mise en forme tableau 2.3.4 • §3.2 Mise à jour champ Subject • §3.3/3.4/3.5 Mise à jour champ Issuer • §3.5 Corection de coquille (REALAUTH/REALCIPHER) • §3.7Mise à jour du champ Subject AltName et Validity pour l'AC REALSSL • §3.8 Mise à jour sur champ Key Usage pour l'AC REALTS • §3.6 Détail du champ Issuer pour l'AC REALTECH
6.0	10/12/2020	ADSN	• Mise à jour certificats de signature des réponses OCSP
7.0	14/01/2021	ADSN	• Mise à jour certificats de signature des réponses OCSP
8.0	22/03/2021	ADSN	• Mise à jour §2.3.6 : suppression du lien des CGU dans les QCStatements.
9.0	Juin 2021	ADSN	• Ajout d'un paragraphe « OID des certificats des AC », • Ajout d'une ligne dans le tableau du paragraphe « Authority Information Access », • Mise à jour des profils « Les certificats du Niveau Autorité de Certification (AC) » : Correction de Authority Information Access qui doit être renseigné à 'Yes'. • Mise à jour du profil « Certificat de la clé de signature pour les Serveurs de signature » de l'AC REALTECH : coquille documentaire : 'SubjectAltName' et 'Utilisation avancée de la clé' : corrigé à « N.U ».
10.0	05/10/2021	ADSN	• Ajout d'un paragraphe sur les contraintes du service OCSP
11.0	Juin 2022	ADSN	• Suppression de REALSSL et REALCIPHER du § 2.3.8 Accès aux informations sur l'autorité • Ajout des profils du certificat de signature serveur SACRE et certificat de chiffrement SACRE • Ajout du profil du certificat d'authentification SSL SACRE
12.0	2023	ADSN	• Mise à jour du logo PUBLIC à la nouvelle charte graphique • Subject/ligne OU : ajout de « ou Non renseigné pour les certificats émis après le 01/09/2022» pour les profils concernés • Ajout de la ville pour les profils concernés • Modification de la ligne O et de la TVA associée pour les profils concernés • Corrections du document (termes manquants dans le tableau de description des certificats concernés): - Key usage :ajout de Dataencipherment - Authority Information access :ajout du service OCSP

Description des certificats et CRL de la chaîne d'AC Notaires de France

SOMMAIRE

Description des certificats et CRL de la chaîne d'AC Notaires de France

1 | Résumé et domaine d'application

Ce document décrit le format des profils des certificats, des CRL (Certificat Revocation List) et de réponses OCSP émis par la PKI du Notariat pour la chaîne d'Autorité de Certification (AC) NOTAIRES DE FRANCE.

2 | Profil (ou gabarit) des certificats X.509 émis par les AC du Notariat

2.1 Schéma du profil de certificat

Certificat				
Contenu du certificat				
Informations de base	Version			Version
	Numéro de série			Serial Number
	Information sur la signature du certificat par l'AC (algorithmes et paramètres)			Signature Algorithm
	Nom de l'émetteur du certificat			Issuer
	Période de validité du certificat			Validity
	Nom du porteur de certificate (DN, contenant le CN du certificat)			Subject
	Information sur la clé publique (valeur de la clé publique, algorithme et paramètre)			Subject Public Key Info
Extensions	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				

2.2 Informations de base

Les informations de base du certificat sont :

- Serial Number : Numéro de série du certificat, identifie de manière unique le certificat dans le système d'une AC.
- Signature Algorithm : Information sur les algorithmes et paramètres de la signature du certificat par l'AC
- Issuer : Nom de l'émetteur du certificat. Ce champ est composé de plusieurs attributs :
- Validity : Période de validité du certificat
- Subject : Nom du porteur de certificat.

Les champs <Issuer> et <Subject> peuvent être composés de plusieurs attributs (dont l'ordre d'apparition n'est pas strucutrant) identifiés par une ou plusieurs lettres qui signifient : **C** = Country / **O** = Organization Name / **OU** = Organizational Unit Name / **UID** =User identifier («**2.5.4.97**» dans ce document) / **CN** = Common Name / **SN** = SurName / **G (ou GN)** = GivenName.

2.3 Extensions standard utilisées dans les certificats X.509 NOTAIRES

2.3.1 BasicConstraints

Cette extension (Contrainte de base) indique si un titulaire peut agir comme une autorité de Certification (AC) en utilisant sa clé privée pour signer les certificats. Cette extension est présente et critique uniquement pour les autorités de certification.

2.3.2 Subject Key Identifier (SKI)

Cette extension (Identificateur de la clé du sujet) identifie la clé publique du certificat. Elle est nécessaire pour utiliser les AKI.

2.3.3 Authority Key Identifier (AKI)

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

2.3.4 CertificatePolicies

Cette extension (Stratégie du certificat) définit les politiques de certification, identifiée par leur OID, que le certificat reconnaît supporter.

2.3.4.1 OID et URL des Politiques de Certification (PC)

Politique de Certification (PC) et son OID	Détail de la structure de l'OID de la PC							URL de la PC
	OID notariat	AC NDF*	Env.*	Document		Id doc		URL de téléchargement pour de la PC
PC NOTAIRES DE FRANCE 1.2.250.1.78.2.1.1.1	1.2.250.1.78	.2	.X	.1		.1		http://www.preuve-electronique.org/PC_NOTAIRESDEFRANCE_1.2.250.1.78.2.1.1.1.pdf
	OID notariat	AC NDF*	Env.*	Sous-AC	Id.AC	Doc.	Id doc	
PC REALSIGN (03/05/2018) 1.2.250.1.78.2.1.3.1.1.4	1.2.250.1.78	.2	.X	.3	.1	.1	.4	http://www.preuve-electronique.org/PC_REALSIGN_1.2.250.1.78.2.1.3.1.1.4.pdf
PC REALAUTH 1.2.250.1.78.2.1.3.2.1.1	1.2.250.1.78	.2	.X	.3	.2	.1	.1	http://www.preuve-electronique.org/PC_REALAUTH_1.2.250.1.78.2.1.3.2.1.1.pdf
PC REALCIPHER 1.2.250.1.78.2.1.3.3.1.1	1.2.250.1.78	.2	.X	.3	.3	.1	.1	http://www.preuve-electronique.org/PC_REALCIPHER_1.2.250.1.78.2.1.3.3.1.1.pdf
PC REALTECH 1.2.250.1.78.2.1.3.4.1.1	1.2.250.1.78	.2	.X	.3	.4	.1	.1	http://www.preuve-electronique.org/PC_AC_REALTECH_1.2.250.1.78.2.1.3.4.1.1.pdf
PC REALTS 1.2.250.1.78.2.1.3.5.1.1	1.2.250.1.78	.2	.X	.3	.5	.1	.1	http://www.preuve-electronique.org/PC_AC_REALTS_1.2.250.1.78.2.1.3.5.1.1.pdf
PC REALSSL 1.2.250.1.78.2.1.3.6.1.1	1.2.250.1.78	.2	.X	.3	.6	.1	.1	http://www.preuve-electronique.org/PC_AC_REALSSL_250.1.78.2.1.3.6.1.1.pdf

*NDF : Notaires de France
*Env. : Environnement, toujours valorisé à « 1 » dans l'environnement de production pour la chaîne d'AC « Notaires de France ».

Description des certificats et CRL de la chaîne d'AC Notaires de France

2.3.4.2 OID des certificats des AC

Ce tableau liste les OID des certificats pour chaque AC, Notaires de France et ses AC Filles.

OID du certificat de l'AC	Détail de la structure de l'OID du certificat de l'AC								
	OID notariat	AC ROOT	Env.*	Id. « Sous-AC »	Id. AC	Id. «Certificat»	Classe	Catégorie	Utilisation
AC NOTAIRE DE FRANCE									
1.2.250.1.78.2.1.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**			**.2**	**.4**	**.3**	**.4**
AC REALSIGN									
1.2.250.1.78.2.1.3.1.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**	**.3**	**.1**	**.2**	**.4**	**.3**	**.4**
AC REALAUTH									
1.2.250.1.78.2.1.3.2.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**	**.3**	**.2**	**.2**	**.4**	**.3**	**.4**
AC REALCIPHER									
1.2.250.1.78.2.1.3.3.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**	**.3**	**.3**	**.2**	**.4**	**.3**	**.4**
AC REALTECH									
1.2.250.1.78.2.1.3.4.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**	**.3**	**.4**	**.2**	**.4**	**.3**	**.4**
AC REALTS									
1.2.250.1.78.2.1.3.5.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**	**.3**	**.5**	**.2**	**.4**	**.3**	**.4**
AC REALSSL									
1.2.250.1.78.2.1.3.6.2.4.3.4	**1.2.250.1.78**	**.2**	**.X**	**.3**	**.6**	**.2**	**.4**	**.3**	**.4**

* Env. : Environnement, toujours valorisé à « 1 » dans l'environnement de production pour la chaîne d'AC « Notaires de France ».

2.3.4.3 OID des certificats utilisateurs (sur clé REAL) émis par une AC Fille

Ce tableau liste les OID des certificats présent sur la clé REAL des utilisateurs.

Utilisation	Certificat pour un Notaire						AC émettrice pour rappel
	OID notariat	Structure OID historique**					
		.AC ROOT	.Env*	.Sous-AC.Id AC (AC Notaires)	.Sous-AC.Id AC (AC REAL)	Certificat.Classe.Catégorie.Utilisation	
Signature d'Acte Authentique (Cert-SA)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.2.4.1	REALSIGN
Signature (Cert-S)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.2.3.1	REALSIGN
Authentification (Cert-A)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.2.3.2	REALAUTH
Chiffrement (Cert-C)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.2.3.3	REALCIPHER
	Certificat pour un Collaborateur						
Signature (Cert-S)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.1.3.1	REALSIGN
Authentification (Cert-A)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.1.3.2	REALAUTH
Chiffrement (Cert-C)	1.2.250.1.78	.1	.X	.3.1	.3.1	.2.1.3.3	REALCIPHER

* Env. : Environnement, toujours valorisé à « 1 » dans l'environnement de production pour la chaîne d'AC « Notaires de France ».

** L'OID des certificats de type porteur conserve pour des raisons techniques, la structure de l'OID de la chaîne d'AC initiale (AC ROOT : Professions Reglementées /Sous-AC AC Notaires /AC REAL). Ceci explique pourquoi les certificats utilisateurs ne porte pas la même strucutre de base que l'OID de l'AC qui les émets.

2.3.4.4 Valeur QCP-n-qscd

Pour les certificats de signature qualifiés émis par l'AC REALSIGN, la valeur QCP-n-qscd (0.4.0.194112.1.2) est positionnée pour indiquer la conformité de la politique de certification aux standards en vigueurs.

2.3.5 Subject Alt Name

Cette extension (autre nom de l'objet) indique l'adresse email. Uniquement pour les titulaires.

Pour l'AC REALSSL, cette extension contient le FQDN (Fully Qualified Domain Name) qui correspond à l'adresse (URL ou IP) pour atteindre le serveur.

2.3.6 Qualified Certificate Statements (1.3.6.1.5.5.7.1.3)

Ces extensions sont ajoutées uniquement aux certificats de signature émis par l'AC REALSIGN. L'extension QC Statement indique que le certificat de signature est qualifié.

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 la bi-clé associée au certificat a été générée par un SSCD.
- Id-etsi-qcs-QcPDS (0.4.0.1862.1.5) : Indique les CGU applicables, avec un lien HTTPS vers ces dernières en anglais, au format PDF/A (uniquement pour REALSIGN 2025). Cet attribut n'est plus utilisé pour les AC postérieures à l'AC REALSIGN 2025.
- Id-etsi-qct-esign (0.4.0.1862.1.6.1) : Indique que le certificat est qualifié pour la signature électronique comme défini dans la réglementation européenne (EU) 910/2014.

2.3.7 KeyUsage (extension toujours marquée critique)

Cette extension (utilisation de la clé), critique, 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)

2.3.8 Authority Information Access (accès aux informations sur l'autorité)

Cette extension définit les différentes méthodes mises en place pour recueillir les informations sur les autorités signataires des certificats uniquement pour les AC : REALSIGN, REALAUTH, REALTECH, REALTS.

- Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : adresse de téléchargement du certificat de l'AC émettrice.
- Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : url d'accès au service OCSP associé au certificat.

AC émettrice	Adresse téléchargement du statut certificat de l'AC émettrice *	URL d'accès au service OCSP associé au cetificat
NOTAIRE DE FRANCE	http://www.preuve-electronique.org/ListeRevocations/notairesdefrance2033.crt	NU**
REALSIGN	http://www.preuve-electronique.org/ListeRevocations/realsignAAAA.crt	http://ocsp.preuve-electronique.org
REALAUTH	http://www.preuve-electronique.org/ListeRevocations/realauthAAAA.crt	http://ocsp.preuve-electronique.org
REALTECH	http://www.preuve-electronique.org/ListeRevocations/realtechAAAA.crt	http://ocsp.preuve-electronique.org
REALTS	http://www.preuve-electronique.org/ListeRevocations/realtsAAAA.crt	http://ocsp.preuve-electronique.org

* AAAA = Année de fin de validité 'AAAA' : REALSIGN AAAA, REALAUTH AAAA, REALTECH AAAA, REALTS AAAA

** Non-Utilisé

3 | Description des profils de certificats pour les différentes AC

« N.U » signifie Non Utilisé.

3.1 Les certificats du Niveau Racine (AC ROOT) « NOTAIRES DE FRANCE »

- Certificat de la Clé de certification (self signed).
- Certificat de signature des ARL.

Objet	Format	Certificat de clé de certification de l'AC ROOT
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 2.5.4.97 = **SI:FR-784350134**, CN = **NOTAIRES DE FRANCE 2033**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 16 ans
Subject	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **SI:FR-784350134 (Pour l'AC ROOT créé avant 2020)**, ou VATFR-67784350134 CN = NOTAIRES DE FRANCE AAAA
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 4096 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		Yes*
Critical	Boolean	True
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* OID et URL de la PC de l'AC NOTAIRES DE FRANCE OID du certificat
SubjectAltName	IA5string	N.U*
Qualified certificate Statements : 1.3.6.1.5.5.7.1.3		N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Key cert Sign, CRLSign**
CrlDistributionPoint		N.U
Authority Information Access		N.U*
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée associée à ce certificat
Utilisation avancée de la clé	Seq	N.U

* (cf §.2.3)

Description des certificats et CRL de la chaîne d'AC Notaires de France

3.2 Les certificats du Niveau Autorité de Certification (AC)

Objet	Format	Certificat de clé de certification Autorité de Certification (AC)
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **SI:FR-784350134,** ou VATFR-67784350134 CN = **NOTAIRES DE FRANCE AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 8 ans
Subject	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = • **SI:FR-784350134**, uniquement pour les AC REAL**SIGN 2025**, REAL**AUTH 2025** et REAL**CIPHER 2025**. • **VATFR-67784350134**, pour les autres AC (REAL**TECH 2025**, REAL**SSL 2025** et REAL**TS 2025)** et toute autre AC créée à partir de 2020. CN = (Nom de l'AC + Année de fin de validité 'AAAA') : REALSIGN AAAA, REALAUTH AAAA, REALCIPHER AAAA, REALTECH AAAA, REALSSL AAAA, REALTS AAAA.
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 4096 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		Yes*
Critical	Boolean	True
Pathlen	Integer	0
Subject Key identifier		Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* OID et URL de la PC de l'AC NOTAIRES DE FRANCE OID du certificat
SubjectAltName	IA5string	N.U*
Qualified certificate Statements : 1.3.6.1.5.5.7.1.3		N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Key cert Sign , CRLSign**
CrlDistributionPoint		Yes
Authority Information Access		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC ROOT
Utilisation avancée de la clé	Seq	N.U

* (cf §.2.3)

3.3 Les certificats du Niveau Utilisateur émis par l'AC REALSIGN

Les certificats de niveau utilisateur sont les suivants :

- Certificat de la clé de signature.

A noter : l'AC REALSIGN émet aussi des certificats signataires de réponse OCSP, pour lesquels le profil est décrit au §3.9.

Objet	Format	Certificat de clé de signature
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **SI:FR-784350134 ou VATFR-67784350134** CN = **REALSIGN AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C=FR, SN=/Nom/, G = /Prénom/, CN = /Nom Prénom (n° de titulaire)/, *Le n° de titulaire est un numéro à 10 chiffres formaté ainsi : [3][CRPCEN de l'office du titulaire] [0][Profil titulaire : Chiffre pair=Notaire/Chiffre impair=Collaborateur][Compteur 00 à 99]*
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier		Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALSIGN – OID du certificat – OID QCP-n-qscd : 0.4.0.194112.1.2
SubjectAltName	IA5string	Email du porteur*
Qualified certificate Statements : 1.3.6.1.5.5.7.1.3	Seq	Yes*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Non repudiation**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realsignAAAA.crl
Authority Information Access		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALSIGN
Utilisation avancée de la clé	Seq	N.U

* (cf §.2.3)

3.4 Les certificats du Niveau Utilisateur émis par l'AC REALAUTH

Les certificats de niveau utilisateur sont les suivants :

- Certificat de la clé d'authentification.

A noter : l'AC REALAUTH émet aussi des certificats signataires de réponse OCSP, pour lesquels le profil est décrit au §3.9.

Objet	Format	Certificat de clé d'authentification
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/20222.5.4.97 = **SI:FR-784350134** ou VATFR-67784350134 CN = **REALAUTH AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = Professions Réglementées, ou CONSEIL SUPERIEUR DU NOTARIAT OU = Notaires ou Non renseigné pour les certificats émis après le 01/09/2022 OU = AC Déléguée ou Non renseigné pour les certificats émis après le 01/09/2022 OU = REAL ou Non renseigné pour les certificats émis après le 01/09/2022 SN=/Nom/, G = /Prénom/, CN = Nom Prénom (n° de titulaire) *Le n° de titulaire est un numéro à 10 chiffres formaté ainsi : [3][CRPCEN de l'office du titulaire] [0][Profil titulaire : Chiffre pair=Notaire/Chiffre impair=Collaborateur][Compteur 00 à 99]*
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALAUTH – OID du certificat
SubjectAltName	IA5string	Email du porteur*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Digital signature**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realauthAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALAUTH
Utilisation avancée de la clé	Seq	Critique /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)

* (cf §.2.3)

3.5 Les certificats du Niveau Utilisateur émis par l'AC REALCIPHER

Les certificats de niveau utilisateur sont les suivants :

- Certificat de la clé de chiffrement.

A noter : l'AC REALCIPHER émet aussi des certificats signataires de réponse OCSP, pour lesquels le profil est décrit au §3.9.

Objet	Format	Certificat de clé de chiffrement
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **SI:FR-784350134** ou VATFR-67784350134 CN = **REALCIPHER AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = Notaires de France ou CONSEIL SUPERIEUR DU NOTARIAT OU = TITULAIRES ou Non renseigné pour les certificats émis après le 01/09/2022 SN=/Nom/, G = /Prénom/, CN = Nom Prénom (n° de titulaire) *Le n° de titulaire est un numéro à 10 chiffres formaté ainsi : [3][CRPCEN de l'office du titulaire] [0][Profil titulaire : Chiffre pair=Notaire/Chiffre impair=Collaborateur][Compteur 00 à 99]*
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALCIPHER – OID du certificate
SubjectAltName	IA5string	Email du porteur*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Key Encipherment, DataEncipherment**
CrlDistributionPoint		Yes http://www.preuve-lectronique.org/ListeRevocations/realcipherAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALCIPHER
Utilisation avancée de la clé	Seq	N.U*

* (cf §.2.3)

3.6 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 signature serveur SACRE
- Certificat de Chiffrement SACRE
- Certificat de la clé de signature pour les serveurs de signature,

A noter : l'AC REALTECH émet aussi des certificats signataires de réponse OCSP, pour lesquels le profil est décrit au §3.9.

3.6.1 Certificat de la clé d'authentification pour les opérateurs

Objet	Format	Certificat de clé d'authentification
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR- 67784350134,** CN = **REALTECH AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT,ou ASSOCIATION POUR LE DEVELOPPEMENT DU SERVICE NOTARIAL OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = VATFR-54329325005 CN = Prénom NOM OPERATEUR Facultatif : (39999701xx) avec xx compris entre 00 et 99
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALTECH – OID du certificate
SubjectAltName	IA5string	Nom principal = /compte de production/ Email du porteur*
Qualified certificate Statements : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Digital Signature**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realtechXXXX.crl
Authority Information Access		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALTECH
Utilisation avancée de la clé	Seq	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)

* (cf §.2.3)

3.6.2 Certificat de signature serveur SACRE

Objet	Format	Certificat de clé de signature
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR- 67784350134,** CN = **REALTECH AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134** CN = Serveur SACRE CMS SIGN ou Serveur SACRE CMS
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 4096 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALTECH – OID du certificat
SubjectAltName	IA5string	N.U*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Non répudiation**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realtechAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALTECH
Utilisation avancée de la clé	Seq	N.U*

* (cf §.2.3)

3.6.3 Certificat de Chiffrement SACRE

Objet	Format	Certificat de clé de signature
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR- 67784350134,** CN = **REALTECH AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134 ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134** CN = Serveur SACRE CMS CHIF
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 4096 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALTECH – OID du certificate
SubjectAltName	IA5string	N.U*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Chiffrement de la clé (KeyEncipherment), Chiffrement des données (dataEncipherment)**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realtechAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALTECH
Utilisation avancée de la clé	Seq	N.U*

* (cf §.2.3)

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

Objet	Format	Certificat de clé de signature
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR- 67784350134,** CN = **REALTECH AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT,ou ASSOCIATION POUR LE DEVELOPPEMENT DU SERVICE NOTARIAL OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134 ou VATFR-54329325005** CN = Serveur de signature – Compteur : 00 à 99
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALTECH – OID du certificat
SubjectAltName	IA5string	N.U*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Digital Signature**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realtechAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALTECH
Utilisation avancée de la clé	Seq	N.U*

* (cf §.2.3)

3.7 Les certificats du Niveau Opérateur ou Serveur émis par l'AC REALSSL

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

- Certificat de la clé d'authentification pour les serveurs SSL ;
- Certificat de la clé d'authentification pour les clients SSL ;
- Certificat d'authentification SSL SACRE

A noter : l'AC REALSSL émet aussi des certificats signataires de réponse OCSP, pour lesquels le profil est décrit au §3.9.

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

Objet	Format	Certificat de clé d'authentification
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = VATFR-67784350134**,** CN = **REALSSL AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 397 jours
Subject	PrintString	C = FR, O = ASSOCIATION POUR LE DEVELOPPEMENT DU SERVICE NOTARIAL OU = 0002 **/N° de SIREN/**, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-54329325005** CN = FQDN du serveur (Ce champ doit correspondre à celui indiqué en Nom alternatif=SubjectAltName) Ville = VENELLES
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALSSL – OID du certificate
SubjectAltName	IA5string	Fully-Qualified Domain Name (FQDN)*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Key Encipherment, DigitalSignature**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realsslAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALSSL
Utilisation avancée de la clé	Seq	Authentification du serveur (1.3.6.1.5.5.7.3.1)

* (cf §.2.3)

3.7.2 Certificat de la clé d'authentification pour les Clients SSL

Objet	Format	Certificat de clé d'authentification
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = VATFR-67784350134, CN = **REALSSL AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 397 jours
Subject	PrintString	C = FR, O = ASSOCIATION POUR LE DEVELOPPEMENT DU SERVICE NOTARIAL OU = 0002 **/N° de SIREN/**, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-54329325005** CN = FQDN du serveur (ce champ doit correspondre à celui indiqué en Nom alternatif=SubjectAltName) Ville = VENELLES
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 4096 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALSSL – OID du certificate
SubjectAltName	IA5string	Fully-Qualified Domain Name (FQDN)*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Key Encipherment, DigitalSignature**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realsslAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALSSL
Utilisation avancée de la clé	Seq	Authentification du client (1.3.6.1.5.5.7.3.2)

* (cf §.2.3)

3.7.3 Certificat d'authentification SSL SACRE

Objet	Format	Certificat de clé d'authentification
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = VATFR-67784350134, CN = **REALSSL AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C = FR, O = CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 Ville= PARIS 2.5.4.97 = **VATFR-67784350134** CN = Serveur SACRE CMS
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 4096 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALSSL – OID du certificat
SubjectAltName	IA5string	Fully-Qualified Domain Name (FQDN)*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Digital signature**
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realsslAAAA.crl
Authority Information Access*		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALSSL
Utilisation avancée de la clé	Seq	Authentification du client (1.3.6.1.5.5.7.3.2)?

* (cf §.2.3)

3.8 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 eIDAS

A noter : l'AC REALTS émet aussi des certificats signataires de réponse OCSP, pour lesquels le profil est décrit au §3.9.

3.8.1 Certificat de la clé de signature pour les Serveurs d'horodatage eIDAS

Objet	Format	Certificat de clé d'horodatage
Certificate	Seq	
TBSCertificate	Seq	
Version	Integer	2 (version 3)
SerialNumber	Integer	Numéro de série aléatoire contenant comme préfixe le condensat du DN de l'AC signataire
Signature	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134,** CN = **REALTS AAAA**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans
Subject	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134,** CN = **ADSN.SDC.UH*X.AAAAMMJJHHMMSS*** (avec X = n° d'identification de l'Unité d'Horodatage concernée et **AAAAMMJJHHMMSS** = date heure de génération du certificat). *A noter : le CN des certificats en 2018 est sous le format : REAL.NOT.SES.UH.X.aaaammjjhhmmss*
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier		Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes* – OID et URL de la PC de l'AC REALTS – OID du certificat
SubjectAltName	IA5string	Email du contact (responsable du certificat)*
Qualified certificate Statements : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Non-repudiation** *A noter :* ce champ est valorisé à 'Digital Signature' pour les certificats générés avant septembre 2020
CrlDistributionPoint		Yes http://www.preuve-electronique.org/ListeRevocations/realtsAAAA.crl
Authority Information Access		Yes* – Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice. – Protocole de statut de certificat en ligne (1.3.6.1.5.5.7.48.1) : donne l'url d'accès au service OCSP associé au certificat.
SignatureAlgorithm	OID	SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC REALTS
Utilisation avancée de la clé	Seq	Critique timestamping (1.3.6.1.5.5.7.3.8)

* (cf §.2.3)

3.9 Les certificats de signature des réponses OCSP

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

- NOTAIRES DE FRANCE
- REALSIGN
- REALAUTH
- REALTECH
- REALTS
- REALSSL
- REALCIPHER

Objet	Format	Certificat de 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 signataire
Signature	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11) ou SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134,** CN = **Voir liste des AC au §3.9**
Validity	UTCTime	Not Before <<date création>> Not After : date création + 3 ans (2 ans pour ceux antérieur à septembre2020)
Subject	PrintString	C=FR, O=CONSEIL SUPERIEUR DU NOTARIAT, OU = 0002 784350134, ou Non renseigné pour les certificats émis après le 01/09/2022 2.5.4.97 = **VATFR-67784350134,** CN = **REAL.NOT.SES.OCSP.*X.AAAAMMJJHHMMSS*** ou **ADSN.SDC.OCSP.Y.X.*AAAAMMJJHHMMSS*** (avec Y = caractère d'identification technique interne et X = nom de l'AC et AAAAMMJJHHMMSS = date heure de génération du certificate, les secondes indiqués par les caractères "SS" ne sont pas obligatoirement indiquées).
SubjectPublicKeyInfo	Seq	Yes
AlgorithmIdentifier	OID	RSA encryption (1.2.840.113549.1.1.1)
SubjectPublicKey	BitString	Longueur du module de la clé publique : 2048 bits Exposant public fixé à 65537
Extensions	Seq	Extension 1.3.6.1.5.5.7.48.1.5 id-pkix-ocsp-nocheck dans les certificats signataires de l'OCSP
BasicConstraint		N.U*
Critical	Boolean	N.U*
Pathlen	Integer	N.U*
Subject Key identifier	Seq	Yes*
Authority Key identifier	Seq	Yes*
Critical	Boolean	No
CertificatePolicy		Yes – OID et URL de l'AC concernée* – OID du certificate*
SubjectAltName	IA5string	N.U*
Qualified certificate Statements* : 1.3.6.1.5.5.7.1.3	Seq	N.U*
Key Usage	Seq	Yes*
Critical	Boolean	True
Value	Bitstring	**Digital signature**
CrlDistributionPoint		Yes
Authority Information Access*		Yes* Autorité de certification émettrice (1.3.6.1.5.5.7.48.2) : donne l'adresse de téléchargement du certificat de l'AC émettrice.
SignatureAlgorithm	OID	SHA-256 avec RSA encryption (1.2.840.113549.1.1.11) ou SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
SignatureValue	BitString	Signature calculée à l'aide de la clé privée de l'AC (256 octets)
Utilisation avancée de la clé	Seq	Signature OCSP (1.3.6.1.5.5.7.3.9)

* (cf §.2.3)

4 | Profil d'une CRL

Toutes les Listes des Certificats Révoqués (LCR, dont l'acronyme anglais CRL est plus souvent utilisé) émis par les AC du Notariat ont le même format, mais les informations peuvent différer.

Le format est le suivant :

<table>
<tr><th colspan="6">CRL</th></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Contenu de la CRL</td></tr>
<tr><td colspan="6">Version</td></tr>
<tr><td colspan="6">Information sur la signature de la LCR par l'AC (algorithmes et paramètres)</td></tr>
<tr><td colspan="6">Nom du fournisseur de la LCR</td></tr>
<tr><td colspan="6">Date d'émission de la LCR</td></tr>
<tr><td colspan="6">Date de la prochaine émission de LCR</td></tr>
<tr><td colspan="6">Numéro de la LCR</td></tr>
<tr><td colspan="6">Liste des certificats révoqués</td></tr>
<tr><td rowspan="5"></td><td rowspan="4">Numéro de série du certificat révoqué</td><td rowspan="4">Date de révocation</td><td colspan="3">Extension d'entrée de LCR</td></tr>
<tr><td>Identifiant du type de l'extension</td><td>Criticité (oui/non)</td><td>Valeur</td></tr>
<tr><td>Identifiant du type de l'extension</td><td>Criticité (oui/non)</td><td>Valeur</td></tr>
<tr><td>…</td><td></td><td></td></tr>
<tr><td rowspan="5">Numéro de série du certificat révoqué</td><td rowspan="5">Date de révocation</td><td colspan="3">Extension d'entrée de LCR</td></tr>
<tr><td>Identifiant du type de l'extension</td><td>Criticité (oui/non)</td><td>Valeur</td></tr>
<tr><td>Identifiant du type de l'extension</td><td>Criticité (oui/non)</td><td>Valeur</td></tr>
<tr><td>…</td><td></td><td></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Algorithme de signature de la LCR</td></tr>
<tr><td colspan="6">Algorithme</td></tr>
<tr><td colspan="6">Paramètres</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Signature numérique du contenu de la LCR</td></tr>
<tr><td colspan="6">Valeur de la signature numérique de la LCR par l'AC</td></tr>
<tr><td colspan="6"></td></tr>
</table>

4.1 Champs et extensions des CRL

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

LA PKI spécifique à l'AC ROOT produit une CRL (ARL) tous les 6 mois, avec une durée de validité de 1 an (lors d'une cérémonie).

Champ	Valeur
Version	V2
Signature	Le champ signatureAlgorithm contient l'identifiant de l'algorithme de signature de la LCR : SHA-512 avec RSA encryption (1.2.840.113549.1.1.13)
Issuer	DN du certificat de l'AC signataire de la liste de révocation.
This Update	Ce champs défini la date et l'heure de l'émission de cette LCR. 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 LCR. Le format UTC Time est utilisé pour ce champ.
Certificats révoqués	Tous les certificats révoqués sont listés (les certificats 'révoqués et non-expirés', également les certificats 'révoqués et expirés'). 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
CRL Number	N° de la LCR
Authority Key Identifier	Cette extension identifie la clé publique à utiliser (empreinte) pour vérifier la signature d'une LCR.
ExpiredCertsOnCRL	Cette extension indique que la LCR contient l'ensemble des certificats révoqués expirés depuis la date de début de validité de l'AC signataire.

5 | Réponses OCSP

5.1 Contraintes du services OCSP

Le service OCSP du Notariat, exposé sur http://ocsp.preuve-electronique.org, est conforme à la RFC 6960. Cependant, certaines contraintes supplémentaires ont été mises en place par le Notariat pour garantir une qualité de service adaptée :

- L'algorithme de hash SHA-1 est strictement interdit sur l'ensemble des champs cryptographiques.
- Le certificat de signature des réponses OCSP est obligatoirement un certificat comportant l'extension de clé d'usage « id-kp-OCSPSigning », et est émis par la même AC ayant émis le certificat à vérifier.
- Il n'est pas possible d'effectuer un appel au service OCSP portant sur plusieurs certificats dans une même requête.

5.2 Profil d'une réponse OCSP

Les réponses OCSP des AC REALSIGN, REALAUTH, REALTECH, REALTS, REALSSL, REALCIPHER et NOTAIRES DE FRANCE sont composées ainsi :

Champ	Valeur
Version	1
ResponseId	DN du certificat de signature de la réponse OCSP
ThisUpdate	Date de production de la demande (GMT)
ProducedAt	Date de production de la réponse (GMT)
NextUpdate	Date de la prochaine mise à jour du statut
ArchiveCutOff	Date de début de validité du certificat de l'AC Signataire
Responses	
Certificate ID	
Hash Algorithm	Sha256 ou SHA512
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/unknow
Revocation time	Si le certificat est révoqué : Date de révocation (GMT)
This update	Identique à la date de production de la réponse
Signature de la réponse	Signature Sha256WithRSAEncryption ou Sha512WithRSAEncryption
Certificate	NA