

# CERTIFICAT DE CONFORMITE

L'organisme certificateur LSTI

Déclare que le prestataire de service de certification électronique

## CRYPTOLOG INTERNATIONAL

SIEGE : 7 RUE DU FAUBOURG POISSONNIERE 75009 PARIS

Délivre des services de confiance<sup>1</sup> conformes au

**Règlement européen 910/2014 du parlement  
européen et du conseil sur l'identification  
électronique et les services de confiance pour les  
transactions électroniques au sein du marché  
intérieur (eIDAS)**

Les services, les certificats et les niveaux certifiés conformes sont détaillés en annexe de la présente attestation.

Ce certificat est enregistré sous le numéro : **Certificate LSTI N° 11050-1072-V1.0**

Ce certificat est basé sur les rapports d'évaluation :

**LSTI 11050-1072\_RA\_eIDAS\_CONF\_v3-0**

**LSTI 11050\_1072\_rapport eval\_complementaire\_pshe**

**LSTI 11050\_1072\_Exigences\_transition\_horodatage**

**LSTI 11050\_1246\_CRYPTOLOG INTERNATIONAL\_eIDAS\_REval\_exigences\_ANSSI\_PSC\_qualifiés\_v3.0**

**LSTI 11050\_1246\_CRYPTOLOG**

**INTERNATIONAL\_eIDAS\_REval\_exigences\_complANSI\_delivrance\_certificats\_qualifiés\_v3.0**

Date de début de validité 24 July 2017

Date de fin de validité 23 July 2019

---

Armelle TROTIN

Directrice de la certification

<sup>1</sup> Selon eIDAS Art.3 (16)

## Annexe 1

### Schéma de certification

#### Accréditation

LSTI est accrédité par le Cofrac sous le numéro n°4-0063 selon la norme NF EN ISO 17021, sous le n° 5-0546 selon la norme NF EN ISO/CEI 17065 :2012 et sous le numéro n° 4-0091 selon la norme NF EN ISO/CEI 17024 et selon les règles d'application du Cofrac pour les portées précises disponibles sur le site [www.cofrac.fr](http://www.cofrac.fr).

Les certificats de conformité sont émis conformément aux règles générales de la certification des Prestataires de services de confiance (PSC) pour le niveau qualifié **LSTI Q053** ou dans le règlement Q055 pour les certifications aux normes européennes listées au paragraphe exigences ci-après.

#### Contexte réglementaire

La certification de conformité est émise dans le cadre des textes législatifs et réglementaires suivants :

- Règlement européen 910/2014 du parlement européen et du conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)

Et ses actes d'exécution.

#### Exigences

Pour le niveau « qualifié » les exigences de conformité sont décrites dans les documents de l'organe de contrôle disponibles sur le site [www.ssi.gouv.fr](http://www.ssi.gouv.fr) :

- [1] Critères d'évaluation de la conformité au règlement eIDAS
- [2] Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - critères d'évaluation de la conformité au règlement eIDAS
- [3] Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité eIDAS au règlement eIDAS
- [4] Services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés
- [5] Services de conservation qualifiés des signatures et des cachets électroniques qualifiés - Critères d'évaluation de la conformité eIDAS au règlement eIDAS
- [6] Services d'envoi recommandé électronique qualifiés - Critères d'évaluation de la conformité eIDAS au règlement eIDAS

La conformité aux textes cités ci-dessus vaut présomption de conformité aux exigences correspondantes du règlement européen 910/2014 :

- Prestataires de services de confiance qualifiés (articles du règlement (UE) n°910/2014 eIDAS : 5(1), 13(2), 15, 19(1), 19(2), 24(2) a à g, 24(2).j)
- Services d'horodatage électronique qualifiés (articles du règlement (UE) n°910/2014 eIDAS : 24(2).e, 24(2).h et i, 42(1). a à c)

- Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site Internet [articles du règlement (UE) n°910/2014 eIDAS : 24(1), 24(2).e, 24(2).h, 24(2).i, 24(2).k, 24(3), 24(4), 28(1), 38(1), 45(1), 28(4), 38(4), 28(5), 38(5)]
- Services de validation de certificats qualifiés de signature électronique et de cachet électronique [articles du règlement (UE) n°910/2014 eIDAS : 24(2).e, 24(2).h, 24(2).i, 32(1), 33(1), 40]
- Services de conservation qualifié de signature et de cachet électronique qualifiés [articles du règlement (UE) n°910/2014 eIDAS : 24(2).e, 24(2).h, 24(2).i, 34(1), 40]
- Services d'envoi recommandé électronique qualifiés [articles du règlement (UE) n°910/2014 eIDAS : 24(2).e, 24(2).h, 24(2).i, 44(1)]

Est vérifiée également la conformité aux normes :

- **EN 319 401** : Signatures électroniques et infrastructures (ESI) - Exigences de politique générale des prestataires de service de confiance
- **EN 319 411-1** : Signatures électroniques et infrastructures (ESI) - Exigences de politique et de sécurité applicables aux prestataires de service de confiance délivrant des certificats - Partie 1 : Exigences générales
- **EN 319 411-2** : Signatures électroniques et infrastructures (ESI) - Exigences de politique et de sécurité applicables aux prestataires de service de confiance délivrant des certificats qualifiés - Partie 2 : Exigences applicables aux prestataires de service de confiance délivrant des certificats qualifiés UE
- **EN 319 421** : Signatures électroniques et infrastructures (ESI) - Exigences de sécurité et de politique des prestataires de service de confiance délivrant des horodatages
- **EN 319 102-1** : Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation
- **ETSI TS 102 640-3**: Technical Specification Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) : Part 3: Information Security Policy Requirements for REM Management Domains

Et aux exigences des schéma(s) de certification

- **Q053** - Règlement de certification des prestataires de services de confiance (PSCO)- Niveau Qualifié
- **Q055** - Règlement de certification des prestataires de services de confiance (PSCO)

## Résultats de l'évaluation de conformité

- Les services listés en annexe 2 sont délivrés conformément aux exigences listées ci-dessus, en fonction du niveau du service.
- Les exigences de la certification décrites dans le schéma de certification sont respectées.

## Acronymes - Services et niveaux

DVCP	Domain Validation Certificate Policy	Authentification serveur
EVCP	Extended Validation Certificate Policy	Authentification serveur

LCP	Lightweight Certificate Policy	Signature-authentication-chiffrement
NCP	Normalized Certificate Policy	Signature-authentication-chiffrement
NCP+	Extended Normalized Certificate	Signature-authentication-chiffrement
OCSF	Online Certificate Status Protocol	
OID	Object Identifier	
OVCP	Organizational Validation Certificate Policy	Authentication serveurur
QCP-l	Policy for EU qualified certificate issued to a legal person	Cachet
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD	Cachet
QCP-n	Policy for EU qualified certificate issued to a natural person	Signature
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD	Signature
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person	Authentication serveurur
QSCD	Qualified electronic Signature/Seal Creation Device	
TSA	Time Stamp Authority	Time Stamp
TSAP	Time Stamp Authority Policy	Time Stamp

## Annexe 2

### Services de certification déclarés conformes

Les services évalués sont caractérisés par les certificats listés ci-après.

CA NAME	Regulation	eIDAS level	RGS Level	Standard	Level	serial number (root) OID (end users)	Service
Universign Hardware CA	UE 910/2014 eIDAS	Level Qualified		EN 319 411-2	QCP-n	1.3.6.1.4.1.15819.5.1.3.1	Signature
Universign hardware CA	UE 910/2014 eIDAS	Non qualified		EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.3.3	Signature
Universign hardware CA	UE 910/2014 eIDAS	Non qualified		EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.3.4	Cachet
Universign hardware CA	UE 910/2014 eIDAS	Level Qualified		EN 319 411-2	QCP-l	1.3.6.1.4.1.15819.5.1.3.5	Cachet
Universign timestamping CA	UE 910/2014 eIDAS	Non qualified	*	EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.1	Cachet
Universign	UE 910/2014 eIDAS	Level Qualified		EN 319 421		1.3.6.1.4.1.15819.5.2.2	Horodatage
Universign Hardware Primary CA	UE 910/2014 eIDAS	Non qualified		EN 319 411-1	NCP+	1.3.6.1.4.1.15819.5.1.2.1	Signature
Universign Software Primary CA	UE 910/2014 eIDAS	Non qualified		EN 319 411-1	NCP	1.3.6.1.4.1.15819.5.1.2.2	Signature

### Suivi des modifications

Version	Date d'émission	Modification
Version 1	24 July 2017	Initiale certification

**FIN DU CERTIFICAT**