CERTIFICAT DE CONFORMITE

L'organisme certificateur LSTI

Déclare que le prestataire de service de certification électronique

DHIMYOTIS

SIEGE : 20, ALLEE DE LA RAPERIE 59650 VILLENEUVE D'ASCQ - FRANCE

Délivre des services de confiance[1] 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° 23–1373-V1.0**

Ce certificat doit être considéré en conjonction avec les rapports d'évaluation :

LSTI 23_1373_Rapport d'audit eIDAS_411-1&2
LSTI 23_1373_Rapport d'horodatage_eIDAS_421
LSTI 23_1373_eidas REval_exigences compl ANSSI_delivrance_certificats_qualifies
LSTI 23_1373_eidas REval_exigences compl ANSSI_horodatage_qualifie
LSTI 23_1373_eidas REval_exigences compl ANSSI_PSC_qualifies
LSTI 23_1373_Rapport d'audit PSCe RGS_e2final_S
LSTI 23_1373_Rapport d'audit PSHe RGS_e2final_S

Date de début de validité 03 mai 2019
Date de fin de validité 02 mai 2021

cofrac ACCRÉDITATION COFRAC N° 5-0546 CERTIFICATION DE PRODUITS ET SERVICES PORTÉE DISPONIBLE SUR WWW.COFRAC.FR

ARMELLE TROTIN ID

Signature numérique de ARMELLE TROTIN ID
DN : c=FR, o=SECURITE TECHNOL L'INFORMATION LSTI SAS, 2.5.4.97=NTRFR-45386786300046, ou=0002 45386786300046, sn=TROTIN, givenName=ARMELLE, cn=ARMELLE TROTIN ID, serialNumber=I11681009
Date : 2019.05.29 10:59:07 +02'00'

Armelle TROTIN
Directrice de la certification

[1] 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.
Les certificats de conformité sont émis conformément aux règles générales de la certification des Prestataires de services de confiance (PSC) **LSTI Q053** 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

Les exigences sont décrites dans les normes suivantes :

- ***EN 319 401 V2.1.1****: Signatures électroniques et infrastructures (ESI) - Exigences de politique générale des prestataires de service de confiance*
- ***EN 319 411-1 V1.1.1****: 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 V2.1.1:*** *Signature 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 V1.1.1****: 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 -eidas

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-authentification-chiffrement
NCP	Normalized Certificate Policy	Signature-authentification-chiffrement
NCP+	Extended Normalized Certificate	Signature-authentification-chiffrement
OCSP	Online Certificate Status Protocol	
OID	Object IDentifier	
OVCP	Organizational Validation Certificate Policy	Authentification serveur
TSA	Time Stamp Authority	Time Stamp
TSAP	Time Stamp Authority Policy	Time Stamp
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	Authentification serveur
QSCD	Qualified electronic Signature/Seal Creation Device	

Annexe 2

Services de certification déclarés conformes

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

CA NAME	Standard	Level	serial number (root) OID (end users)	Service
Certigna Root CA				Root
Certigna Entity CA	EN 319 411-1	LCP	1.2.250.1.177.2.6.1.1.1	Cachet
Certigna Entity CA	EN 319 411-1	LCP	1.2.250.1.177.2.6.1.3.1	Cachet
Certigna Entity CA	EN 319 411-2	QCP-1 + QsealCD	1.2.250.1.177.2.6.1.4.1	Cachet
Certigna Entity CA	EN 319 411-2	QCP-1 + QSealCD	1.2.250.1.177.2.6.1.6.1	Cachet
Certigna Entity CA	EN 319 411-2	QCP-I + QSealCD	1.2.250.1.177.2.6.1.41.1	Cachet
Certigna Entity CA	RGS	**	1.2.250.1.177.2.6.1.42.1	Cachet
Certigna Entity Code Signing CA	EN 319 411-1	LCP	1.2.250.1.177.2.8.1.1.1	Cachet
Certigna Entity Code Signing CA	EN 319 411-2	QCP-1 + QSealCD	1.2.250.1.177.2.8.1.2.1	Cachet
Certigna Identity CA	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.1.1	Encryption
Certigna Identity CA	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.2.1	Authentication & signature
Certigna Identity CA	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.3.1	Encryption
Certigna Identity CA	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.4.1	Authentication & signature
Certigna Identity Plus CA	EN 319 411-2	QCP-n-QSignCD	1.2.250.1.177.2.4.1.1.1	Authentication & Signature
Certigna Identity Plus CA	EN 319 411-1	NCP+	1.2.250.1.177.2.4.1.2.1	Authentication
Certigna Identity Plus CA	EN 319 411-2	QCP-n-QSignCD	1.2.250.1.177.2.4.1.3.1	Signature
Certigna Identity Plus CA	EN 319 411-2	QCP-n-QSignCD	1.2.250.1.177.2.4.1.4.1	Authentication & Signature
Certigna Identity Plus CA	EN 319 411-1	NCP+	1.2.250.1.177.2.4.1.5.1	Authentication
Certigna Identity Plus CA	EN 319 411-2	QCP-nQSignCD	1.2.250.1.177.2.4.1.6.1	Signature
Certigna Services CA	EN 319 411-1	OVCP	1.2.250.1.177.2.5.1.1.1	Authentication server
Certigna Services CA	EN 319 411-1	OVCP	1.2.250.1.177.2.5.1.2.1	Authentication server
Certigna Services CA	EN 319 411-2	QCP-W	1.2.250.1.177.2.5.1.3.1	Server-Authentication
Certigna Service CA	EN 319 411-1	EVCP	1.2.250.1.177.2.5.1.3.1	Server-Authentication
Certigna Wild CA	EN 319 411-1	OVCP	1.2.250.1.177.2.7.1.1.1	Authentication server
Certigna Wild CA	EN 319 411-1	OVCP	1.2.250.1.177.2.7.1.2.1	Authentication server
FR03-Certigna Cachet Serveur	EN 319 411-1	NCP+ 2D doc	1.2.250.1.177.2.2.1.1	Cachet
Service d'horodatage	EN 319 421		1.2.250.1.1777.2.9.1	Time-stamp

Suivi des modifications

Version	Date d'émission	Modification
Version 1	03 mai 2019	Initiale certification

FIN DU CERTIFICAT