CERTIFICATE OF CONFORMITY

The certification body LSTI

declares

CERTSIGN

SIÈGE : BULEVARDUL TIMISOARA 5A BUCHAREST - ROMANIA

Provides trust electronic services[1] that comply with

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Appendix to this certificate provide the list of services, certificates and level of compliance.

The present certificate is registered under N° : **Certificate LSTI N° 1612-10-V1.0**

The present certificate is valid only in conjunction with the conformity assessment report(s)
1612_10_AInit421_GB_S.pdf
1612_10_audit stage 2 report eidas_411-2_S.pdf

ARMELLE TROTIN
ID
2017.07.27 19:05:58
+0200
Signé par Armelle Trotin

Starting date 27 June 2017
Expiring date 26 June 2019

Armelle TROTIN
Head of the Certification Body

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

[1] eIDAS Art.3 (16)

Appendix 1

Certification Scheme

LSTI SAS has been accredited pursuant to the accreditation certificate of French Accreditation Body COFRAC with registration number 5-0546 rév. 3 dated 21 April 2017in accordance with NF EN ISO/IEC 17065:2013 as a certification body for products, processes, and services in accordance with the Annex of the accreditation certificate and in accordance with the eIDAS EU Regulation Art. 3 (18) and the ETSI EN 319 403 (details on www.cofrac.fr). The certification scheme is described in document LSTI-Q055- eIDAS certification rules.

Requirements

Requirements for Trust Service Providers are specified in REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC:

- General provisions Art.: 5(1)),
- Trust services-General provisions Art.13(2), 15,
- Trust services – Supervision Art.19(1), 19(2),
- Qualified trust services Art. 20, 21 (1) and (3), 23(1),23(2) , 24(1), 24(2), 24(3), 24(4),
- Qualified certificates for electronic signatures Art.: 28, 29(1), Annex I,
- Qualified certificates for electronic seals Art. 38(1), 39(1), 39(2), Annex III,
- Qualified certificates for website authentication Art.45(1), Annex IV,
- Qualified electronic time stamps Art.: 42(1)
- Validation of qualified electronic signatures Art.: 32(1), 34, 40
- Qualified validation service for qualified electronic signatures Art. 32(1), 33, 34, 40,
- Qualified preservation service for qualified electronic signatures Art.: 34(1), 40
- Validation and preservation of qualified electronic seals Art. 40
- Qualified electronic registred delivery services Art.: 24(2).e, 24(2).h, 24(2).i, 44(1)

And verified in assessing, in particular, the conformity to:

- **EN 319 403 V2.2.2**: *Electronic Signatures and infrastructures (ESI) - Trust Service Providers conformity assessment - Requirements for conformity assessment bodies assessing Trust Service Providers*
- **EN 319 401 V2.1.1**: *Electronic Signatures and Infrastructures (ESI) – General Policy requirements for trust service providers*
- **EN 319 411-1 V1.1.1**: *Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements*
- **EN 319 411-2 V2.1.1**: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*
- **EN 319 421 V1.1.1**: *Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers issuing time- stamps*
- **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*

And

- **Q055**_eIDAS certification rules

Conformity Assessment Results

- The target of conformity assessment (appendix 2) meets the criteria required under the regulation depending of the level of the service.
- The certification requirements defined in the certification scheme are fulfilled.

Abbreviations - Services et level

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
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	
TSA	Time Stamp Authority	Time Stamp
TSAP	Time Stamp Authority Policy	Time Stamp

Appendix 2

Conformity assessment Target

The target of conformity assessment is characterized by the certificate information of the inspected trust services:

CA NAME	Regulation	eIDAS level	Standard	Level	serial number (root) OID (end users)	Service
certSIGN ROOT CA G2						Root
certSIGN Qualified CA	UE 910/2014 eIDAS				2.5.29.32.0	Sub CA
certSIGN Qualified CA	UE 910/2014 eIDAS	Level qualified	EN 319 411-2	QCP-n-QSCD	1.3.6.1.4.1.25017.3.1.3.1	Signature KS
certSIGN Qualified CA	UE 910/2014 eIDAS	Level qualified	EN 319 411-2	QCP-n-QSCD	1.3.6.1.4.1.25017.3.1.3.2	Signature KC
certSIGN Qualified CA	UE 910/2014 eIDAS	Level qualified	EN 319 411-2	QCP-l-qscd	1.3.6.1.4.1.25017.3.1.3.3	Seal KS
certSIGN Qualified CA	UE 910/2014 eIDAS	Level qualified	EN 319 411-2	QCP-l-qscd	1.3.6.1.4.1.25017.3.1.3.4	Seal KC
certSIGN Qualified CA	UE 910/2014 eIDAS	Level qualified	EN 319 411-2	QCP-l-qscd	1.3.6.1.4.1.25017.3.1.3.5	Seal KC Timestamping
certSIGN Qualified CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	NCP+	1.3.6.1.4.1.25017.3.1.3.6	OCSP
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	NCP+	2.5.29.32.0	Sub CA
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.1	Signature-Authentication KS
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.2	Signature-Authentication TKS

CA NAME	Regulation	eIDAS level	Standard	Level	serial number (root) OID (end users)	Service
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.3	Signature-Authentication TKC
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.4	Signature-Authentication KC
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.5	Encryption KS
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.6	Encryption TKS
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.7	Encryption TKC
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.8	Encryption KC
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.9	Seal KS
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.10	Seal TKS
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.11	Seal TKC
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.12	Seal KC
certSIGN Public CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	NCP	1.3.6.1.4.1.25017.3.1.2.13	OCSP
certSIGN Web CA					2.5.29.32.0	Sub CA
certSIGN Web CA	UE 910/2014 eIDAS	Level qualified	EN 319 411-2	QCP-w EVCP	1.3.6.1.4.1.25017.3.1.4.1	Server-Authentication
certSIGN Web CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	OVCP	1.3.6.1.4.1.25017.3.1.4.2	Server-Authentication
certSIGN Web CA	UE 910/2014 eIDAS	Non qualified	EN 319 411-1	NCP+	1.3.6.1.4.1.25017.3.1.4.3	OCSP

Declaration of conformity modifications records

Version	Issuing Date	Changes
Version 1	27 June 2017	Initiale certification

END OF THE CERTIFICAT