CONFORMITY ASSESSMENT BODY
EIDAS
TRUST SERVICE PROVIDERS
ISO 27001
LA ISO 27001
LI ISO 27001
RM ISO 27005

Audit Attestation for

CERTSIGN

Reference: No. 1612-52-AL-V2.0

Saint-Malo, 23rd July 2018

To whom it may concern,

This is to confirm that LSTI has successfully audited the CAs of the CERTSIGN without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number n°1612-52-AL-V2.0 and consist of 8 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

LSTI Group
10 Avenue Anita Conti
35400 Saint-Malo, France
E-Mail: atrotin@lsti.eu
Phone: +33 608675144

With best regards,

ARMELLE TROTIN ID
Signature numérique de ARMELLE TROTIN ID
Date : 2018.07.25 09:38:45 +02'00'

Armelle Trotin
Head of Certification Body

Identification of the conformity assessment body (CAB):	LSTI[1],10 Avenue Anita Conti, 35400 Saint-Malo, France registered under n°453867863 Accredited by COFRAC under registration number 5-0546 in accordance with EN ISO/IEC 17065:2013 and in accordance with the eIDAS EU Regulation art. 3 (18) and the ETSI EN 319 403 v2.2.2. Detailed scope at *http://cofrac.fr/en/easysearch/index.php*

Identification of the trust service provider (TSP):	CERTSIGN Bulevardul Timișoara 5A, București 061301, Romania registered under n° J40/484/2006

Identification of the audited Root-CA:	*CERTSIGN Root CA G2*	
	Distinguished Name	*Root CA G2*
	SHA-256 fingerprint	657CFE2FA73FAA38462571F332A2363A 46FCE7020951710702CDFBB6EEDA3305
	Certificate Serial number	110034B64EC6362D36
	Applied policy	None
	Validity	*notBefore=Feb 6 09:27:35 2017 GMT* *notAfter=Feb 6 09:27:35 2042 GMT*

Identification of the audited Root-CA:	*CERTSIGN Qualified CA*	
	Distinguished Name	*CERTSIGN Qualified CA*
	SHA-256 fingerprint	C670C79BF277AF7E7B34A6AA4FA3044418 33C6BD01A70A7E9B7E9B7A2D94C1C1F926
	Certificate Serial number	*1002A980FB5F4585DD08*
	Applied policy	X509v3 Any Policy
	Validity	*notBefore=Feb 6 10:06:03 2017 GMT* *notAfter=Feb 6 10:06:03 2027 GMT*

[1] in the following termed shortly "*CAB*"

Identification of the audited Root-CA:	*CERTSIGN Public CA*	
	Distinguished Name	*CERTSIGN Public CA*
	SHA-256 fingerprint	9917BFD853738985E46C920419410E96 6C316982769E71817E27D0384BBE3679
	Certificate Serial number	*1001660345DD0680E322*
	Applied policy	Any Policy
	Validity	*notBefore=Feb 6 09:52:49 2017 GMT* *notAfter=Feb 6 09:52:49 2027 GMT*

Identification of the audited Root-CA:	*CERTSIGN Web CA*	
	Distinguished Name	*CERTSIGN Web CA*
	SHA-256 fingerprint	F114469FB80778133A1F70E4D8338EDA B97DD42CEB8ECC01CAFB70D6B87DF11E
	Certificate Serial number	10034B8E66F50920F6C5
	Applied policy	Any Policy
	Validity	*notBefore=Feb 6 10:18:16 2017 GMT* *notAfter=Feb 6 10:18:16 2027 GMT*

The audit was performed as full annual audit at the TSP's location in *Bucarest, Romania*. It took place from *26/03/2018* until *29/03/2018* and covered the period from *14/04/2017* until *29/03/2018*. The audit was performed according to the European Standards "*ETSI EN 319 411-2, V2.1.1 (2016-02)", "ETSI EN 319 411-1, V1.1.1 (2016-02)"* as well as CA Browser Forum Requirements "*EV SSL Certificate Guidelines, version 1.6.6" and "Baseline Requirements, version 1.5.1"* considering the requirements of the "*ETSI EN 319 403, V2.2.2 (2015-08)*" for the Trust Service Provider Conformity Assessment.

The full annual audit was based on the following policy and practice statement documents of the TSP:

- certSIGN_ROOT_CA_CPS_EN_v2.2 for its root CA,
- certSIGN_PUBLIC_CA_CPS_v2.3 refers to Lightweight Certificate Policy with or without a secure user device,
- certSIGN_QUALIFIED_CA_CPS_v2.5 refers to the certificate policy for EU qualified certificates or qualified seals, issued to natural or legal persons with private key related to the certified public key in a QSCD,
- certSIGN_WEB_CA_OV_SSL_CPS_v1.3 refers to the certificate policy for OV (Organizational Validation) SSL certificates,
- CPS-QCW-SSL-v1.4 refers to the certificate policy for EU qualified website authentication certificates.

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

Identification of the Sub-CA	Distinguished Name	Certificate Serial number OID	Applied policy	Service	EKU
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.194112.1.2 1.3.6.1.4.1.25017.3.1.3.1	EN 319 411-2 QCP-n-QSCD	Signature KS	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.194112.1.2 1.3.6.1.4.1.25017.3.1.3.2	EN 319 411-2 QCP-n-QSCD	Signature KC	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.194112.1.1 1.3.6.1.4.1.25017.3.1.3.3	EN 319 411-2 QCP-l	Seal KS	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.194112.1.1 1.3.6.1.4.1.25017.3.1.3.4	EN 319 411-2 QCP-l	Seal KC	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.194112.1.1 1.3.6.1.4.1.25017.3.1.3.5 *Not audited*	EN 319 421 TSA	Seal KS Timestamping	Time stamping
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.2042.1.2 1.3.6.1.4.1.25017.3.1.3.6 *Not audited*	EN 319 411-1 NCP+	OCSP	OCSP Signing
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.1	EN 319 411-1 LCP	Signature-Authentication KS	Secured Email (S/MIME) Client Authentication (without Server Authentication)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.2	EN 319 411-1 LCP	Signature-Authentication TKS	Secured Email (S/MIME) Client Authentication (without Server Authentication)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.3	EN 319 411-1 LCP	Signature-Authentication TKC	Secured Email (S/MIME) Client Authentication (without Server Authentication)

Identification of the Sub-CA	Distinguished Name	Certificate Serial number OID	Applied policy	Service	EKU
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.4	EN 319 411-1 LCP	Signature-Authentication KC	Secured Email (S/MIME) Client Authentication (without Server Authentication)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.5	EN 319 411-1 LCP	Encryption KS	Secured Email (S/MIME)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.6	EN 319 411-1 LCP	Encryption TKS	Secured Email (S/MIME)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.7	EN 319 411-1 LCP	Encryption TKC	Secured Email (S/MIME)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.8	EN 319 411-1 LCP	Encryption KC	Secured Email (S/MIME)
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.9	EN 319 411-1 LCP	Seal KS	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.10	EN 319 411-1 LCP	Seal TKS	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.13 *Not audited*	EN 319 411-1 LCP	OCSP	OCSP Signing
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.12	EN 319 411-1 LCP	Seal KC	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing

Identification of the Sub-CA	Distinguished Name	Certificate Serial number OID	Applied policy	Service	EKU
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.1 1.3.6.1.4.1.25017.3.1.2.11	EN 319 411-1 LCP	Seal TKC	Secured Email (S/MIME) Client Authentication (without Server Authentication) Document Signing
certSIGN Web CA	certSIGN Web CA	0.4.0.194112.1.4 0.4.0.2042.1.4 1.3.6.1.4.1.25017.3.1.4.1	EN 319 411-2 QCP-w-EVCP	Server-Authentication	Server Authentication (EV) and Client Authentication only
certSIGN Web CA	certSIGN Web CA	0.4.0.2042.1.7 1.3.6.1.4.1.25017.3.1.4.2	EN 319 411-1 OVCP	Server-Authentication	Server Authentication (non EV) and Client Authentication only
certSIGN Web CA	certSIGN Web CA	0.4.0.2042.1.2 1.3.6.1.4.1.25017.3.1.4.3 *Not audited*	EN 319 411-1 NCP+	OCSP	OCSP Signing

Table 1: Sub-CA's issued by the Root-CA

Modifications records

Version	Issuing Date	Changes
Version 1	27 June 2018	Initial attestation
Version 2	23 July 2018	Fingerprint SHA-256 corrections

End of the audit attestation letter