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

Audit Attestation for

CertSIGN

Reference: No. LSTI_AAL_1612-163_V0.1 - DRAFT

Saint-Malo, 22 April 2020

To whom it may concern,

This is to confirm that LSTI has audited the CAs of CertSIGN without critical findings.
This present Audit Attestation Letter is registered under the unique identifier number n°1612-163 and consist of 10 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-Mails: pbouchet@lsti.fr & cabforum@acab-c.com
Phone: +33 6 33 38 80 78

With best regards,

_____
Philippe Bouchet
Director

Identification of the conformity assessment body (CAB):	LSTI[1] SAS, 10 Avenue Anita Conti, 35400 Saint-Malo - France registered under n°453867863 LSTI Worldwide Limited, Clifton House – Fitzwilliam street lower Dublin 2 – Ireland registered under n°582309 Accredited by COFRAC under registration number 5-0546 in accordance with EN ISO/IEC 17065:2012 and in accordance with the eIDAS EU Regulation art. 3 (18) and the ETSI EN 319 403 v2.2.2. Detailed scope at https://www.cofrac.fr/ Attestation of accreditation link: https://tools.cofrac.fr/annexes/sect5/5-0546.pdf [2] COFRAC 52 Rue Jacques Hillairet 75012 Paris FRANCE Phone: +33 144688220

Identification of the trust service provider (TSP):	CertSIGN S.A. AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29, Bucharest Registered in Romania under number J40/484/2006
Audited sites:	CA/RA - AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29, Bucharest

Identification of the audited Root-CA:	certSIGN ROOT CA G2	
	Distinguished Name	certSIGN ROOT CA G2
	Certificate Serial Number	110034B64EC6362D36
	SHA-256 fingerprint	657CFE2FA73FAA38462571F332A2363A46FCE7020951710702CDFBB6EEDA3305
	Validity	Not Before=Feb 6 09:27:35 2017 GMT Not After=Feb 6 09:27:35 2042 GMT

1 in the following termed shortly "*CAB*"

2 URL to the accreditation certificate hosted by the national accreditation body

Identification of the audited Root-CA:	certSIGN Public CA	
	Distinguished Name	certSIGN Public CA
	Certificate Serial Number	1001660345DD0680E322
	SHA-256 fingerprint	9917BFD853738985E46C920419410E966C316982769E71817E27D0384BBE3679
	Validity	notBefore=Feb 6 09:52:49 2017 GMT notAfter=Feb 6 09:52:49 2027 GMT

Identification of the audited Root-CA:	CERTSIGN Qualified CA	
	Distinguished Name	CERTSIGN Qualified CA
	Certificate Serial Number	1002A980FB5F4585DD08
	SHA-256 fingerprint	C670C79BF277AF7E7B34A6AA4FA304441833C6BD01A70A7E9B7A2D94C1C1F926
	Validity	notBefore=Feb 6 10:06:03 2017 GMT notAfter=Feb 6 10:06:03 2027 GMT

Identification of the audited Root-CA:	*CERTSIGN Web CA*	
	Distinguished Name	*CERTSIGN Web CA*
	Certificate Serial Number	*10034B8E66F50920F6C5*
	SHA-256 fingerprint	F114469FB80778133A1F70E4D8338EDAB97DD42CEB8ECC01CAFB70D6B87DF11E
	Validity	notBefore=Feb 6 10:18:16 2017 GMT notAfter=Feb 6 10:18:16 2027 GMT

The audit was performed as full period of time audit at the TSP's location in Bucharest, Romania. It took place from 2020-02-10 until 2020-02-14 and covered the period from 2019-02-15 until 2020-02-14.
The audit was performed as a full audit and has been documented in a specific report.
The next assessment has to be successfully carried out before 2021-02-14 in order to issue a new audit attestation letter as stated in the corresponding certificates issued by LSTI.
The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.2.2 (2018-04)", "ETSI EN 319 411-1, V1.2.2 (2018-04)" and "ETSI EN 319 401, V2.2.1 (2018-04)" as well as CA Browser Forum Requirements "EV SSL Certificate Guidelines, version 1.7.1" and "Baseline Requirements, version 1.6.7" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.
The audit was based on the following policy and practice statement documents of the TSP:

1. [CPS] Certification Practice Statement CERTSIGN ROOT CA G2, Version 2.14, Date: 5 February 2020
2. [CPS] Certification Practice Statement certSIGN QUALIFIED CA, Version 2.22, Date: 7 February 2020
3. [CPS] Certification Practice Statement certSIGN PUBLIC CA, Version 2.12, Date: 7 February 2020
4. [CPS] Certification Practice Statement certSIGN Web CA for Qualified Website Authentication Certificates, Version 1.14, Date: 7 February 2020
5. [CPS] Certification Practice Statement certSIGN Web CA for OV SSL, Version 1.12, Date: 7 February 2020
6. [PDS] PKI Disclosure Statement for certSIGN ROOT CA G2 Hierarchy, Version 2.15, Date: 5 February 2020

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in table 1 and that been covered in this audit.
No major non-conformities have been identified during the audit.

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

- REQ-7.8-06 – Documentation shall be improved

Findings with regard to ETSI EN 319 411-1:

- REG-6.3.1-01 – Implementation shall be improved
- GEN-6.5.1-04 - Implementation shall be improved

Findings with regard to ETSI EN 319 411-2:

- SDP-6.5.1-02 - Implementation shall be improved
- GEN-6.6.1-05 – Documentation shall be improved
- CSS-6.3.10-13 – Documentation shall be improved

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as documented under :
https://bugzilla.mozilla.org/show_bug.cgi?id=1551375
The remediation measures taken by Certsign as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Identification of the Sub-CA	Distinguished Name	Certificate Serial number Applied Policy 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*	*0.4.0.194112.1.2* *1.3.6.1.4.1.25017.3.1.3.2.1*	*EN 319 411-1* *QCP-n-QSCD*	*Remote Signature TKC*	*TLS Web Client Authentication* *E-mail Protection* *Signer of documents*
certSIGN Qualified CA	*certSIGN Qualified CA*	*0.4.0.194112.1.2* *1.3.6.1.4.1.25017.3.1.3.2.2*	*EN 319 411-1* *QCP-n-QSCD*	*Remote Signature TKC (can be used only in the relationships between the Subject and the Subscriber)*	*TLS Web Client Authentication* *E-mail Protection* *Signer of documents*
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*	*0.4.0.194112.1.2* *1.3.6.1.4.1.25017.3.1.3.4.1*	*EN 319 411-1* *QCP-n-QSCD*	*Remote Seal TKC*	*TLS Web Client Authentication* *E-mail Protection* *Signer of documents*
certSIGN Qualified CA	certSIGN Qualified CA	0.4.0.194112.1.1 1.3.6.1.4.1.25017.3.1.3.5	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	EN 319 411-1 NCP+	OCSP	OCSP Signing

Identification of the Sub-CA	Distinguished Name	Certificate Serial number Applied Policy OID	Applied policy	Service	EKU
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.1	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)
certSIGN Public CA	*certSIGN Public CA*	*0.4.0.2042.1.3* *1.3.6.1.4.1.25017.3.1.2.3.1*	*EN 319 411-1 LCP*	*Remote Signature-Authentication TKC*	*TLS Web Client Authentication* *E-mail Protection* *Signer of documents*
certSIGN Public CA	*certSIGN Public CA*	*0.4.0.2042.1.3* *1.3.6.1.4.1.25017.3.1.2.3.2*	*EN 319 411-1 LCP*	*Remote Signature Authentication TKC (can be used only in the relationships between the Subject and the Subscriber)*	*TLS Web Client Authentication* *E-mail Protection* *Signer of documents*
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)

Identification of the Sub-CA	Distinguished Name	Certificate Serial number Applied Policy OID	Applied policy	Service	EKU
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.9	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	0.4.0.2042.1.1 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 Public CA	*certSIGN Public CA*	*0.4.0.2042.1.3* *1.3.6.1.4.1.25017.3.1.2.11.1*	*EN 319 411-1* *LCP*	*Remote Seal TKC*	*TLS Web Client Authentication* *E-mail Protection* *Signer of documents*
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
certSIGN Public CA	certSIGN Public CA	0.4.0.2042.1.3 1.3.6.1.4.1.25017.3.1.2.13	EN 319 411-1 LCP	OCSP	OCSP 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	EN 319 411-1 NCP+	OCSP	OCSP Signing

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

Modifications record

Version	Issuing Date	Changes
Version 1	2020-04-22	Initial attestation

End of the audit attestation letter.