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_1612-231_V1.0

Saint-Malo, 2022-05-12

To whom it may concern,

This is to confirm that LSTI SAS has audited the CAs of CertSIGN without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number 1612-231 and consists of 16 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

Philippe Bouchet
Director

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Identification of the conformity assessment body (CAB) and assessment organization:	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 and qualification of the audit team:	• Number of team members: 2 • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly

1 in the following termed shortly "*CAB*"

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

	available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See "Additional competences of team members" above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: none. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. Auditors code of conduct incl. independence statement:

	Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management:	• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

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

Audit Period covered for all policies:	2021-02-14 to 2022-02-13
Audit dates:	2022-02-15 to 2022-02-18
Audit Location:	CA/RA - AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29A, Bucharest

Identification of the audited Root-CA:	certSIGN ROOT CA G2	
	Distinguished Name	OU = certSIGN ROOT CA G2 O = CERTSIGN SA C = RO
	SHA-256 fingerprint	657CFE2FA73FAA38462571F332A2363A46FCE7020951710702CDFBB6EEDA3305
	Certificate Serial number	110034B64EC6362D36
	Applied policy	ETSI EN 319 411-1 V1.2.2, all policies ETSI EN 319 411-2 V2.2.2, all policies

Identification of the audited Sub-CA:	certSIGN Public CA	
	Distinguished Name	2.5.4.97 = VATRO-18288250 CN = certSIGN Public CA O = CERTSIGN SA C = RO
	SHA-256 fingerprint	9917BFD853738985E46C920419410E966C316982769E71817E27D0384BBE3679
	Certificate Serial number	1001660345DD0680E322
	Applied policy	ETSI EN 319 411-1 V1.2.2; LCP

Identification of the audited Sub-CA:

certSIGN Qualified CA

Identification of the audited Sub-CA:	certSIGN Qualified CA	
	Distinguished Name	2.5.4.97 = VATRO-18288250 CN = certSIGN Qualified CA O = CERTSIGN SA C = RO
	SHA-256 fingerprint	C670C79BF277AF7E7B34A6AA4FA304441833C6BD01A70A7E9B7A2D94C1C1F926
	Certificate Serial number	1002A980FB5F4585DD08
	Applied policy	ETSI EN 319 411-1 V1.2.2; NCP+ ETSI EN 319 411-2 V2.2.2; QCP-N, QCP-L, QCP-N-QSCD, QCP-L-QSCD

Identification of the audited Sub-CA:	certSIGN Web CA	
	Distinguished Name	2.5.4.97 = VATRO-18288250 CN = certSIGN Web CA O = CERTSIGN SA C = RO
	SHA-256 fingerprint	F114469FB80778133A1F70E4D8338EDAB97DD42CEB8ECC01CAFB70D6B87DF11E
	Certificate Serial number	10034B8E66F50920F6C5
	Applied policy	ETSI EN 319 411-1 V1.2.2; NCP+, OVCP, EVCP ETSI EN 319 411-2 V2.2.2; QCP-W

The audit was performed as full 10 days in total including 7 days on site at the TSP's location in Bucharest Romania. It took place from 2022-02-15 until 2022-02-18 and covered the period from 2021-02-14 until 2022-02-13. 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, V2.3.1 (2018-04)" as well as CA Browser Forum Requirements "EV SSL Certificate Guidelines, version 1.7.8" and "Baseline Requirements, version 1.8.1" considering the requirements of the "ETSI EN 319 403-1 V2.3.1 (2020-06)" and "ETSI TS 119 403-2 V1.2.4 (2020-11)" for the Trust Service Provider Conformity Assessment.

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

Certification Practice Statement CERTSIGN ROOT CA G2, Version 2.20, Date: 31 January, 2022
Certification Practice Statement certSIGN QUALIFIED CA, Version 2.32, Date: January 31, 2022
Certification Practice Statement, certSIGN PUBLIC CA, Version2.17, Date: January 31, 2022
Certification Practice Statement, certSIGN Web CA for Qualified Website Authentication Certificates, Version 1.21, Date: January 31, 2022
Certification Practice Statement, certSIGN WebCA for OV SSL, Version1.18, Date: January 31, 2022
PKI Disclosure Statement for certSIGN ROOT CA G2 Hierarchy Version 2.20 Date: January 31, 2022
TERMS AND CONDITIONS regarding the provision of certification services for Website Authentication – QCW, Version 1.4 dated 22.03.2019
TERMS AND CONDITIONS regarding the provision of certification services for Website Authentication – OV SSL, Version 2.2 dated 22.03.2019
TERMS AND CONDITIONS regarding the provision of certification services for Website Authentication – QWAC, v1.5 July 31, 2020
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, Version 1.3 29.05.2020 (Sign QSCD Remote)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, v1.1 jan. 2021 (Seal QSCD Remote)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, v1.2 jan.2021 (Seal QSCD DPSD2)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, Version 3.2 dated 25.05.2020 (Sign QSCD)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, Version: 1.0 – 7 Jan.2021 (Sign QSCD)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, v3.2 ian.2021 (Seal QSCD)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, v1.1 jan.2021 (Sign no QSCD)
TERMS AND CONDITIONS regarding the provision of certification services for qualified certificates according to Regulation (EU) No. 910/2014, v1.1 Jan.2021 (Seal no QSCD)
TERMS AND CONDITIONS regarding the provision of certification services for digital certificates according to Regulation (EU) No. 910/2014, v1.1 11 Nov, 2020 (Sign Remote)
TERMS AND CONDITIONS regarding the provision of certification services for digital certificates according to Regulation (EU) No. 910/2014, v1.3 11 Nov, 2020 (Seal, Remote seal)
TERMS AND CONDITIONS regarding the provision of certification services for digital certificates according to Regulation (EU) No. 910/2014, v2.3- 31 Jan.2022 (Sign, Encryption, with / without hardware device)

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-7.7-01– Implementation shall be improved
- REQ-7.9-11– Implementation shall be improved

Findings with regard to ETSI EN 319 411-1:

- DIS-6.1-02– Implementation shall be improved
- REQ-7.6-01– Implementation shall be improved
- OVR-6.4.8-13– Documentation shall be improved

Findings with regard to ETSI EN 319 411-2:

- GEN-6.6.1-02 – Implementation 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.

During the audited period certSIGN had no bugs in Bugzilla within the scope of this audit.

The Sub-CA 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 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

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
2.5.4.97 = VATRO-18288250 CN = certSIGN Public CA O = CERTSIGN SA C = RO	9917BFD853738985E46C920419410E966C316982769E71817E27D0384BBE3679	ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.1 (Signature-Authentication KS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.2 (Signature-Authentication TKS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.3 (Signature-Authentication TKS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.3.1 (Remote Signature-Authentication TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.3.2 (Remote Signature Authentication TKC - *can be used only in the relationships between the Subject and the Subscriber*)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.4 (Signature-Authentication KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.5 (Encryption KS)	1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.6 (Encryption TKS)	1.3.6.1.5.5.7.3.4 (E-mail Protection)

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.7 (Encryption TKC)	1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.8 (Encryption KC)	1.3.6.1.5.5.7.3.4 (E-mail Protection)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.9 (Seal KS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.10 (Seal TKS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.11 (Seal TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.11.1 (Remote Seal TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.12 (Seal KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.13 (OCSP)	1.3.6.1.5.5.7.3.9 (OCSP Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.14 (Remote Signature TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-1 V1.2.2, LCP (0.4.0.2042.1.3) 1.3.6.1.4.1.25017.3.1.2.15 Authentication Signing and email Protection KC Without HW device	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
2.5.4.97 = VATRO-18288250 CN = certSIGN Qualified CA O = CERTSIGN SA C = RO	C670C79BF277AF7E7B34A6AA4FA304441833C6BD01A70A7E9B7A2D94C1C1F926	ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.1 (Signature KS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.2 (Signature KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.2.1 (Remote Signature TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.2.2 (Remote Signature TKC - *can be used only in the relationships between the Subject and the Subscriber*)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
		ETSI EN 319 411-2 V2.2.2, QCP-L-QSCD (0.4.0.194112.1.3) 1.3.6.1.4.1.25017.3.1.3.3 (Seal KS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-L-QSCD (0.4.0.194112.1.3) 1.3.6.1.4.1.25017.3.1.3.4 (Seal KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-L-QSCD (0.4.0.194112.1.3) 1.3.6.1.4.1.25017.3.1.3.4.1 (Remote Seal TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 421 V1.1.1, TSA, ETSI EN 319 411-2 V2.2.2, QCP-L (0.4.0.194112.1.1) QCP-L-QSCD (0.4.0.194112.1.3) 1.3.6.1.4.1.25017.3.1.3.5 (Seal KS Timestamping)	1.3.6.1.5.5.7.3.8 (Time Stamping)
		ETSI EN 319 411-1 V1.2.2, NCP+ (0.4.0.2042.1.2) 1.3.6.1.4.1.25017.3.1.3.6 (OCSP)	1.3.6.1.5.5.7.3.9 (OCSP Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.7 (Signature KC - *for signing Trusted Lists*)	0.4.0.2231.3.0 (TSL Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-N (0.4.0.194112.1.0) 1.3.6.1.4.1.25017.3.1.3.8 (Signature KS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
		ETSI EN 319 411-2 V2.2.2, QCP-N (0.4.0.194112.1.0) 1.3.6.1.4.1.25017.3.1.3.9 (Signature KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-L-QSCD (0.4.0.194112.1.3) 1.3.6.1.4.1.25017.3.1.3.10 (Remote Seal TKC – PSD2)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-L (0.4.0.194112.1.1) 1.3.6.1.4.1.25017.3.1.3.11 (Seal KS)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-L (0.4.0.194112.1.1) 1.3.6.1.4.1.25017.3.1.3.12 (Seal KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-L (0.4.0.194112.1.1) 1.3.6.1.4.1.25017.3.1.3.13 (Seal KS – PSD2)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
		ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.14 (Signature KC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
		ETSI EN 319 411-2 V2.2.2, QCP-N-QSCD (0.4.0.194112.1.2) 1.3.6.1.4.1.25017.3.1.3.15 (Signature TKC)	1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.7.3.4 (E-mail Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)
2.5.4.97 = VATRO-18288250 CN = certSIGN Web CA O = CERTSIGN SA C = RO	F114469FB80778133A1F70E4D8338EDAB97DD42CEB8ECC01CAFB70D6B87DF11E	ETSI EN 319 411-1 V1.2.2, EVCP (0.4.0.2042.1.4), ETSI EN 319 411-2 V2.2.2, QCP-W (0.4.0.194112.1.4), 1.3.6.1.4.1.25017.3.1.4.1 (Server-Authentication)	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication)
		ETSI EN 319 411-1 V1.2.2, NCP+ (0.4.0.2042.1.2), OVCP (0.4.0.2042.1.7) 1.3.6.1.4.1.25017.3.1.4.2 (Server-Authentication)	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication)
		ETSI EN 319 411-1 V1.2.2, NCP+ (0.4.0.2042.1.2) 1.3.6.1.4.1.25017.3.1.4.3 (OCSP)	1.3.6.1.5.5.7.3.9 (OCSP Signing)
		ETSI EN 319 411-1 V1.2.2, EVCP (0.4.0.2042.1.4) ETSI EN 319 411-2 V2.2.2, QCP-W (0.4.0.194112.1.4) 1.3.6.1.4.1.25017.3.1.4.4 (Server-Authentication – PSD2)	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication)

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

Modifications record

Version	Issuing Date	Changes
Version 1.0	2022-05-12	Initial attestation

End of the audit attestation letter.