



TLS EV Audit Attestation for

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE, S.A.

Reference: PSC-2020-0004

Madrid, 2024-12-16

To whom it may concern,

This is to confirm that AENOR INTERNACIONAL, S.A.U. has audited the CAs of the ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE, S.A. without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "PSC-2020-0004" multiple Root-CAs and consists of 9 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

AENOR INTERNACIONAL, S.A.U.
Génova, 6. 28004 Madrid. España
E-Mail: info@aenor.com
Phone: 91 432 60 00

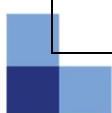
With best regards,

Rafael GARCÍA MEIRO
CEO
2024-12-16





<p>Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:</p>	<ul style="list-style-type: none"> • AENOR CONFÍA, S.A. Génova, 6. 28004 Madrid. España. www.aenor.com • Accredited by ENAC under registration 01/C-PR329 for the certification of trust services according to “UNE-EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)” respectively. Attestation of accreditation link: https://www.enac.es/documents/7020/5ae31445-73fa-4e16-acc4-78e079375c4f • Insurance Carrier (BRG section 8.2): MAPFRE • Third-party affiliate audit firms involved in the audit: none
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> • Number of team members: 1 Lead auditor and 2 auditors • 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 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: <ol style="list-style-type: none"> 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;





	<p>e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls.</p> <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.
<p>Identification and qualification of the reviewer performing audit quality management:</p>	<ul style="list-style-type: none"> 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.
<p>Identification of the CA / Trust Service Provider (TSP):</p>	<p>ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE, S.A. BEATO TOMAS DE ZUMARRAGA 71 01008 VICTORIA GASTEIZ SPAIN</p>
<p>Type of audit:</p>	<p><input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input checked="" type="checkbox"/> Period of time, full audit</p>
<p>Audit period covered for all policies:</p>	<p>2023-10-31 to 2024-10-30</p>



AENOR

Audit Attestation IZENPE SA, PSC-2020-0004



Audit dates:	2024-10-14 to 2024-11-04
Audit location:	CA/RA - BEATO TOMAS DE ZUMARRAGA 71 01008 VICTORIA GASTEIZ SPAIN

.



Root 1: IZENPE.COM

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.5.1 (2023-10)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• EV Guidelines for TLS Server Certificates, version 2.0.1• Baseline Requirements for TLS Server Certificates, version 2.0.8• Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.3.1 (2023-03)
-----------------------	---

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

1. (CPS) Declaración de Prácticas de Certificación version 7.7 as of 2024-11-08
2. (CP) Política de certificados sitio web versión 2.3 as of 2024-10-07

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as documented under

- Bug Izenpe: Not allowed Qualifier ID OID on Certificate Policies extension:
https://bugzilla.mozilla.org/show_bug.cgi?id=1876565
- Bug Izenpe: Failure to Submit Annual CCADB Self-Assessment:
https://bugzilla.mozilla.org/show_bug.cgi?id=1883493
- Bug Izenpe: Duplicate attribute in Subject:
https://bugzilla.mozilla.org/show_bug.cgi?id=1921254
- Bug Izenpe: Not allowed Qualifier ID OID on Certificate Policies extension of Precertificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1922844

The remediation measures taken by Izenpe as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.



Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, O = IZENPE S.A., CN = IZENPE.COM	2530CC8E98321502BAD96F9B1FBA1B099E2D299E0F4548BB914F363BC0D4531F	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, EVCP

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
C = ES, O = IZENPE S.A., OU = BZ Ziurtagiri publikoa - Certificado publico EV, CN = CA de Certificados SSL EV	DB476339CCBFCC9E4BD1D6CB606CA27F00679E1EF8A581E7236309B9D63FFE37	ETSI EN 319 411-2 V2.4.1, QEVCP-W ETSI EN 319 411-1 V1.3.1, EVCP	not defined

Table 2: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit





Root 2: ROOT CA SSL IZENPE 2024

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.5.1 (2023-10)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• EV Guidelines for TLS Server Certificates, version 2.0.1• Baseline Requirements for TLS Server Certificates, version 2.0.8• Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.3.1 (2023-03)
-----------------------	---

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

3. (CPS) Declaración de Prácticas de Certificación version 7.7 as of 2024-11-08
4. (CP) Política de certificados sitio web versión 2.3 as of 2024-10-07

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as described in the following.

- There are no reported or active incidents during the audit period.





Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, O = IZENPE S.A., CN = ROOT CA SSL IZENPE 2024	85F3BB368DA5EA445875794705111A363909279EDA3B319532E0518C13AC2E24	ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP

Table 3: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
C = ES, O = IZENPE S.A., organizationIdentifier = VATES-A01337260, CN = SUBCA SSL 2024	B87F2CA5AD30259FF3E5588DE131C3626D5727CAE24F9BC9B007026DBCC2D652	ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP	serverAuth 1.3.6.1.5.5.7.3.1 clientAuth 1.3.6.1.5.5.7.3.2

Table 4: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit





Modifications record

Version	Issuing Date	Changes
Version 1	2024-12-16	Initial attestation

End of the audit attestation letter.

