Audit Attestation for

Financijska agencija

Reference: AAL14386307rev02

Ljubljana, 2023-06-23

06/23/2023

To whom it may concern,

This is to confirm that “Bureau Veritas d.o.o.” has audited the CAs of the “Financijska agencija” without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “AAL14386307rev02” covers a single Root-CA and consists of 8 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Bureau Veritas d.o.o.
Linhartova cesta 49a
1000 Ljubljana, Slovenia
E-Mail: eidas-slovenia@bureauveritas.com
Phone: +38614757670

With best regards,

Digitally signed by MARKO KOREN
Date: 2023.09.13 15:29:07 +02'00'

Marko Koren
LTM

Digitally signed by BORUT MLAKAR
Date: 2023.09.13 15:43:01 +02'00'

Borut Mlakar
Certification Manager

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• Bureau Veritas d.o.o., Linhartova cesta 49a, 1000 Ljubljana, Slovenia, https://www.bureauveritas.si/sites/g/files/zypfnx291/files/media/document/AAL14386307rev02_1.pdf registered under company_registration no.: 5000939000 • Accredited by Slovenska Akreditacija (SA) https://www.slo-akreditacija.si/?lang=en# under registration accreditation_registration : http://www.slo-akreditacija.si/acreditation/bureau-veritas-d-o-o-3/ [1] for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”. • Insurance Carrier (BRG section 8.2): Zavarovalnica Triglav • Third-party affiliate audit firms involved in the audit: None.
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 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;

[1] URL to the accreditation certificate hosted by the national accreditation body

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 CA / Trust Service Provider (TSP):	Financijska agencija, Ulica grada Vukovara 70, 10000 Zagreb, Croatia, registered under company registration No: 85821130368

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2022-06-03 to 2023-06-02 06/03/2022 to 06/02/2023
Point in time date:	none, as audit was a period of time audit
Audit dates:	2023-05-02 to 2023-05-05 (on site) 05/02/2023 to 05/05/2023 (on site)
Audit location:	Financijska agencija, Ulica grada Vukovara 70, 10000 Zagreb, Croatia CA, PKI, Koturaška 43, 10000 Zagreb, Croatia Poslovnica 9, Ul.kralja Zvonimira 54, 10000 Zagreb, Croatia Poslovnica Varaždin, Augusta Cesarca 2, 42000 Varaždin, Croatia

	DR Ul. Matije Gupca 46, 49210 Zabok, Croatia Poslovnica Vrbovec, Brdo 3, 10340 Vrbovec, Croatia Poslovnica Rijeka, F. Kurelca 3, 51000 Rijeka, Croatia Poslovnica Martinkovac, Martinkovac 127, 51000 Rijeka, Croatia

Root 1: Fina Root CA

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.2.1 (2021-05) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.4.1 (2018-04) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.7.9 ☒ Baseline Requirements, version 1.8.4 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI EN 319 403-1 V2.3.1 (2020-06) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

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

1. FINA Certificate Policy and Certification Practice Statement for Fina Root CA, version 2.8, as of 2023-06-26
2. FINA Certificate Policy for Qualified Certificates for Electronic Signatures and Seals, version 2.0, as of 2023-06-26
3. FINA Certificate Policy for Qualified Certificates for Website Authentication, version 1.5, as of 2023-06-26
4. FINA Certificate Policy for Non-Qualified Certificates, version 1.7, as of 2023-06-26
5. FINA Certificate Policy for Certificates for Website Authentication, version 1.9, as of 2023-06-26
6. FINA Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals, version 2.0, as of 2023-06-26
7. FINA Certification Practice Statement for Qualified Certificates for Website Authentication, version 1.5, as of 2023-06-26
8. FINA Certification Practice Statement for Non-Qualified Certificates, version 1.7, as of 2023-06-26
9. FINA Certification Practice Statement for Certificates for Website Authentication, as of 1.9, version 2023-06-26
10. FINA Qualified Time-Stamp Policy, version 1.8, as of 2023-06-26
11. FINA Qualified Time-Stamping Practice Statement, version 1.8, as of 2023-06-26
12. FINA Certificate Profiles Aligned with The Regulation (EU) No 910/2014 (eIDAS), version 2.3, as of 2023-06-26

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

Findings with regard to ETSI EN 319 401:

7.3 Asset management

7.3.1 General requirements

The QTSP not maintain an inventory of all information assets. [REQ-7.3.1-02]

The organization did not provide an appropriate up-to-date record of information assets in RA. [REQ-7.3.1-02]

7.6 Physical and environmental security

The QTSP not assure that controls are implemented to avoid compromise or theft of information and information processing facilities. [REQ-7.6-04]

The QTSP has not implemented activities to avoid loss, damage or compromise of assets and interruption to business activities. [REQ-7.6-04]

7.7 Operation security

The organization did not ensure consistency or updating of relevant documentation with respect to changes in the application. [REQ-7.7-01]

7.8 Network security

The organization did not provide regular penetration tests of the Source code of critical applications for the operation of the TSP. [REQ-7.8-14]

7.10 Collection of evidence

The QTSP not assure that precise time of significant TSP's environmental and clock synchronization events are recorded. [REQ-7.10-05]

7.13 Compliance

The organization has not provided fully EU and National evidence of the implementation of the legislation in relation to all the trust services it offers in the market. [REQ-7.13-02]

The organization was not providing consistent versioning of documentation related to provide trust services. [REQ-7.13-02]

Findings with regard to ETSI EN 319 411-1:

6.3.4 Certificate acceptance

A QTSP not assure that any person seeking to use a qualified trust service before entering into a contractual relationship, inform, in a clear and comprehensive manner any limitations on its use. [REG-6.3.4-02]

6.4.6 Records archival

The QTSP made uncontrolled change on record of electronic signature delivery confirmation. [OVR-6.4.6-01]

Findings with regard to ETSI EN 319 411-2:

None.

All non-conformities have been closed before the issuance of this attestation.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN = Fina Root CA, O = Financijska agencija, C = HR	5AB4FCDB180B5B6AF0D262A2375A2C77D25602015D96648756611E2E78C53AD3	ETSI EN 319 411-2 V2.2.2, QCP-l-qscd

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
CN = Fina RDC 2015, O = Financijska agencija, C = HR	857BFCE43B1BB4601FF4543B46D3FB2E213BF9B4FEEB6F13BE9EF45C04FF6F8B	[ETSI EN 319 411-1] Policy: LCP; NCP; NCP+; OVCP [ETSI EN 319 411-2] Policy: QCP-n; QCP-l; QCP-n-qscd; QCP-l-qscd; QCP-w; QCP-w-psd2	not defined
CN = Fina RDC 2020, O = Financijska agencija, C = HR	4140B70629FDA4B8A36FD53FB0AA53237157869931B8B2308FD05DF3FF7D78AB	[ETSI EN 319 411-1] Policy: LCP; NCP [ETSI EN 319 411-2] Policy: QCP-l	not defined
CN = Fina RDC-TDU 2015, O = Financijska agencija, C = HR	0AAFB78343B530BA0617C09A70AB285B304259F496E019AFEF8408F2A6DD00F3	ETSI EN 319 411-1] Policy: NCP+ [ETSI EN 319 411-2] Policy: QCP-n; QCP-l; QCP-n-qscd; QCP-l-qscd	not defined

Table 2: 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	2023-06-23	Initial attestation
Version 2	2023-09-11	Corrected 2022-05-03 to 2022-06-03 and added US date format

End of the audit attestation letter.