TAYLLORCOX s.r.o.

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK
TAYLLORCOX PCEB, CAB No. 3239, accredited in accordance with ČSN EN ISO/IEC 17065:2013 by Czech Accreditation Institute (Certificate of accreditation No.: 91/2020, website: www.cai.cz/?subjekt=3239-tayllorcox-s-r-o&lang=en)
Address: Na Florenci 1055/35, Praha 1 - Nové Město, CZ 110 00, info@tayllorcox.com

AUDIT STATEMENT REPORT - I.CA ETSI ASSESSMENT 2020

RSA ALGORITHM

Part I: Basic information

Conformity assessment body (CAB, auditor name):

TAYLLORCOX PCEB,
TAYLLORCOX s.r.o.
Identification No.: 279 02 587
Na Florenci 1055/35
Praha 1 - Nové Město
CZ 110 00
Czech Republic

Audit team: Ing. Martin Dudek (Lead auditor)
Ing. Radek Nedvěd (Head of CAB)

Identification of the trust service provider (CA name):

První certifikační autorita a.s. (hereinafter I.CA)
Identification No.: 264 39 395
Podvinný mlýn 2178/6
Praha 9 - Libeň
CZ 190 00
Czech Republic

Identification of the audited Root CA:

Subject Distinguished Name	CN = **I.CA Root CA/RSA** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 00
SHA-256 fingerprint	d3 d6 07 a9 ff 24 a1 95 23 b6 da 9d 2c 64 94 46 f8 78 8c b9 6d 9f d1 30 97 2e 12 0c 13 67 77 30
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+, DVCP, OVCP, EVCP ETSI EN 319 411-2 V2.2.2 (2018-04) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w

Part II: Conformity evaluation of service

ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

and

ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

PART III: AUDIT INFORMATION

1.1 Audit period

The audit was performed as **full annual audit**, the audit period covered:

Audit period start date: 10/05/2019

Audit period end date: 09/05/2020

1.2 Audit scope

1.2.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

compliance with:

1. ETSI EN 319 411-2 V2.2.2 (2018-04) policies:
    a) QCP-n Policy for EU qualified certificate issued to a natural person (for electronic signatures)
    b) QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (for qualified electronic signatures)
    c) QCP-l Policy for EU qualified certificate issued to a legal person (for electronic seals)
    d) QCP-l Policy for EU qualified certificate issued to a legal person (for electronic seals) + PSD2
    e) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (for qualified electronic seals)
    f) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (for qualified electronic seals) + PSD2
    g) QCP-w: Policy for EU qualified certificates for website authentication
    h) QCP-w: Policy for EU qualified certificates for website authentication + PSD2

2. ETSI EN 319 411-1 V1.2.2 (2018-04) policies:
    a) NCP: Normalized Certificate Policy
    b) NCP+: Enhanced Normalized Certificate Policy requiring a secure cryptographic device
    c) DVCP: Domain Validation Certificate Policy for TLS/SSL certificates
    d) OVCP: Organizational Validation Certificate Policy for TLS/SSL certificates
    e) EVCP: Extended Validation Certificate Policy for TLS/SSL certificates

The system consists of off-line root certification authority (I.CA Root CA/RSA) issuing certificates for subordinate CAs (I.CA SSL EV CA/RSA, I.CA SSL CA/RSA, I.CA Qualified CA/RSA, I.CA Qualified 2 CA/RSA, I.CA TSACA/RSA and I.CA Public CA/RSA), these subordinate CAs are issuing certificates for end users.

The TSP assures that no other non-revoked Sub-CA's technically capable of issuing SSL/TLS certificates have been issued by this Root-CA.

1.2.2 INFORMATION SECURITY RISK ANALYSIS

Information security risk analysis of trustworthy systems supporting "Hierarchical certificate issuing and management system" performed as a part of ETSI EN 319 411-1 and ETSI EN 319 411-2 requirements.

1.3 Audit requirements

1.3.1 Certification services provided by I.CA hierarchical structure of I.CA CAs

1. ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (policies NCP, NCP+, DVCP, OVCP, EVCP)
3. ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QCP-w)
4. ETSI TS 119 495 V1.4.1 (2019-11) Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366 (policy QCP-w-psd2)
5. ETSI EN 319 412, Part 1 to Part 4 (2016-02), Part 5 (2020-04), Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
6. CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", version 1.7.0
7. CA/Browser Forum: "Guidelines For The Issuance And Management Of Extended Validation Certificates", version 1.7.2
8. CEN/TS 419261 March 2015 Security requirements for trustworthy systems managing certificates and timestamps
9. ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.3.2 I.CA's information security risk analysis

1. ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
2. ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
3. ISO/IEC 27002:2013 Information technology Security techniques - Information security management systems -Code of practice for information security controls

1.4 Audit targets

1.4.1 CERTIFICATION SERVICES PROVIDED BY HIERARCHICAL STRUCTURE OF I.CA CAs

A. I.CA Root CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Root CA/RSA** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 00
SHA-256 fingerprint	d3 d6 07 a9 ff 24 a1 95 23 b6 da 9d 2c 64 94 46 f8 78 8c b9 6d 9f d1 30 97 2e 12 0c 13 67 77 30
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+, DVCP, OVCP, EVCP ETSI EN 319 411-2 V2.2.2 (2018-04) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)" „The Root Qualified Certification Authority Certification Policy (RSA Algorithm)“ "Certifikační prováděcí směrnice (algoritmus RSA)" “The Certification Practice Statement (RSA Algorithm)”

B. I.CA SSL EV CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA SSL EV CA/RSA 10/2017** O = První certifikační autorita, a.s. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 fe
SHA-256 fingerprint	75 f5 c8 db 96 b8 e2 14 8a 6a 95 8a 47 83 11 f0 5c 75 8f b7 d9 6d 5b 8b c0 4e 5b 9d 35 9c 3b 09
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policy EVCP ETSI EN 319 411-2 V2.2.2 (2018-04) policy QCP-w
Policy and practice statement documents of the TSP (versions valid within audit period)	“Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (algoritmus RSA)” "Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám PSD2[1] (algoritmus RSA)" “Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)” "Certifikační prováděcí směrnice (algoritmus RSA)"

C. I.CA SSL CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA SSL CA/RSA 07/2015** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 ea
SHA-256 fingerprint	92 a4 46 d2 78 94 31 22 7f f4 b3 34 18 9a a5 a7 b9 30 20 08 ac 37 47 e9 68 c6 ae 68 ad 7a eb 66
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies DVCP and OVCP
Policy and practice statement documents of the TSP (versions valid within audit period)	“Certifikační politika vydávání SSL certifikátů (algoritmus RSA)” “Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)” "Certifikační prováděcí směrnice (algoritmus RSA)"

[1] ETSI TS 119 495 V1.4.1 (2019-11) Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

D. I.CA Qualified CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Qualified CA/RSA 07/2015** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 ec
SHA-256 fingerprint	de 2e a0 58 39 b8 2d ca 52 83 a6 04 c7 d8 df f9 47 f5 46 95 bb b4 da fb 96 48 40 b1 e6 11 da 7e
Applied policy requirements	EN 319 411-2 V2.2.2 (2018-04) policies QCP-n-qscd, QCP-l-qscd
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů SK pro elektronické podpisy (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných mandátních certifikátů SK (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě SK (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

E. I.CA Qualified 2 CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Qualified 2 CA/RSA 02/2016** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 ee
SHA-256 fingerprint	07 6a bc 22 69 32 7e ef 50 0a 0c 57 52 72 62 ba c8 31 f9 d2 df 4e f2 d4 39 e7 4c e1 70 36 aa 3a
Applied policy requirements	ETSI EN 319 411-2 V2.2.2 (2018-04) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)" "Certifikační politika vydávání systémových certifikátů (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě PSD2[1] (algoritmus RSA)" „Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy na dálku (algoritmus RSA)" „Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

F. I.CA TSACA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA TSACA/RSA 05/2017** O = První certifikační autorita, a.s. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 f4
SHA-256 fingerprint	4a b8 bc 60 61 74 3e 09 80 bf d1 21 37 0a 88 c5 11 c4 f2 9e b4 bc 08 97 65 88 6b 64 c7 91 f7 68
Applied policy requirements	ETSI EN 319 411-2 V2.2.2 (2018-04) policy QCP-l
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

G. I.CA Public CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Public CA/RSA 07/2015** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 eb
SHA-256 fingerprint	97 38 4d 1e 5a a6 37 ac 60 1b 19 89 37 15 9f e8 b3 9a 2f d2 9f e4 1a 86 a0 93 0b 65 60 76 6a 71
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)" "Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA)" „Certifikační politika vydávání komerčních certifikátů pro systém elektronické identifikace (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

1.4.2 I.CA's information security risk analysis

The target of audit, the I.CA's Information security risk analysis of trustworthy systems supporting "Hierarchical certificate issuing and management system", is described by the information contained in the internal, I.CA classified, documentation:

Approach to the information security risk assessment and treatment:

"Přístupy k posuzování a ošetřování rizik bezpečnosti informací - důvěryhodné systémy", version 3.3 as of 27/09/2019, I.CA

Scope of the information security management system (ISMS):

"Rozsah ISMS - důvěryhodné systémy", version 5.4 as of 16/09/2019, I.CA

Information security risk assessment and treatment:

"Analýza rizik - Důvěryhodné systémy Závěrečná zpráva", version 1.0 as of September 2019, I.CA

"Výběr protiopatření - důvěryhodné systémy", version 1.5 as of 17/04/2020, I.CA

"Zbytková rizika - důvěryhodné systémy", version 2.5 as of 18/04/2020, I.CA

As a part of the process of continuous improvement of provided services, the company První certifikační autorita, a.s. was assessed for the compliance of the internal implementation of Information Security Management System (ISMS) with the requirements of ISO/IEC 27001:2013 by the independent external audit last year. The scope of ISMS of the company První certifikační autorita, a.s. includes the usage of all internal systems used on the provision of trust services within the meaning of the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) activities. The result of the audit is Certificate No. 1912059861, valid until 20.11.2022.

1.5 Audit workflow

Schedule of audit:

Date	Activity
30/04/2020 – 05/05/2020	Stage 1 audit – verification of I.CA's documentation Location: Office of Auditor (TAYLLORCOX PCEB)
12/05/2020	Stage 2 audit – on site audit Location: Headquarters and operational premises of I.CA company
14/05/2020 – 15/05/2020	Audit Statement Report, Qualifying Attestation Letter Location: Office of Auditor (TAYLLORCOX PCEB)

Methodology:

1. ETSI EN 319 403 V2.3.0 (2019-11): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider
   Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers"
2. ETSI TS 119 403-2 V1.2.1 (2019-04) "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates"
3. ETSI TS 119 403-3 V1.1.1 (2019-03) "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers"
4. ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services.

Documentation and procedures:
Policies and practices that rule the provision and operation of the certification services
Policies and practices to the information security risk assessment and treatment

Part IV: Audit conclusion

Auditor confirms that the examination of I.CA's "Hierarchical certificate issuing and management system" supporting RSA algorithm (chapter 1.4.1) and "Information security risk analysis of its supporting trustworthy systems" (chapter 1.4.2) was conducted in accordance with ETSI standards, in particular EN 319411-1, EN 319411-2, EN 319 403 and, where applicable, has considered all current requirements of ETSI TS 119 495 and CA/Browser Forum Requirements.

The results of examination based on auditor's observations, review of relevant documentation (including web www.ica.cz) and test of administrative and operational procedures and implemented respective controls concluded to the auditor's statement that audited certification services of the company První certifikační autorita, a.s.

comply

with requirements of ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements and of ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

Part V: Signature and confirmation of audit report

Signature of lead auditor:

Ing. Martin Dudek

Praha: 18/05/2020

Ing. Martin Dudek Ing. Martin Dudek 2020.05.18 08:44:28 +02'00'