TAYLLORCOX s.r.o.

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK
TAYLLOR & COX PCEB, certification body 3239, accredited in accordance with ČSN EN ISO/IEC 17065:2013 by Czech Accreditation Institute (Certificate of accreditation No.: 67/2017, website: www.cai.cz/en/Subjekt.aspx?ID=11346)
Address: Na Florenci 1055/35, Praha 1 - Nové Město, CZ 110 00, info@tayllorcox.com

AUDIT STATEMENT REPORT – I.CA ROOT CA/RSA

Part I: Basic information

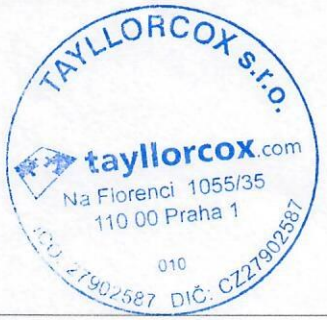
Organization:	První certifikační autorita a.s. (hereinafter I.CA) Identification No.: 264 39 395 Podvinný mlýn 2178/6 Praha 9 - Libeň CZ 190 00 Czech Republic
Auditor:	TAYLLOR & COX s.r.o., TAYLLOR & COX PCEB Identification No.: 279 02 587 Na Florenci 1055/35 Praha 1 - Staré Město CZ 110 00 Czech Republic
Audit team:	Ing. Martin Dudek (Lead auditor) Ing. Radek Nedvěd

Part II: Conformity evaluation of service

ETSI EN 319 411-1 V1.1.1 (2016-02) 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 V2.1.1 (2016-02) 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 scope

1.1.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM" – PART EV SSL CERTIFICATES AND QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION COMPLYING WITH:

1. ETSI EN 319 411-1 V1.1.1 (2016-02) policy: EVCP (Extended Validation Certificate Policy)
2. ETSI EN 319 411-2 V2.1.1 (2016-02) policy: QCP-w (Policy for EU qualified website authentication certificates issued to a legal person)

The hierarchical structure of the system consists of off-line root certification authority (I.CA Root CA/RSA) issuing certificates for 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 CAs are issuing certificates for end users. The target of this audit is I.CA SSL EV CA/RSA only.

1.1.2 INFORMATION SECURITY RISK ANALYSIS:

Trustworthy systems supporting "Hierarchical certificate issuing and management system" as a part of ETSI EN 319 411-1 and ETSI EN 319 411-2 requirements.

1.2 Audit requirements

1.2.1 Certification services provided by I.CA SSL EV CA/RSA as a part of hierarchical structure of I.CA CAs

1. ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
3. ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (policy EVCP)
4. ETSI EN 319 411-2 V2.1.1 (2016-02) 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 (policy QCP-w)
5. ETSI EN 319 412-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

6. ETSI EN 319 412-4 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
7. ETSI EN 319 412-5 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
8. CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"
9. CA/Browser Forum: "Guidelines For The Issuance And Management Of Extended Validation Certificates".
10. CEN/TS 419261 March 2015 Security requirements for trustworthy systems managing certificates and timestamps
11. ETSI TS 119 312 V1.2.1 (2017-05) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
12. ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services.

1.2.2 I.CA's information security risk analysis

1. ETSI EN 319 411-1 V1.1.1 (2016-02) 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 V2.1.1 (2016-02) 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

1.3 Audit targets

1.3.1 CERTIFICATION SERVICES PROVIDED BY I.CA SSL EV CA/RSA AS A PART OF HIERARCHICAL STRUCTURE OF I.CA CA

A. **I.CA Root CA/RSA**

B. **I.CA SSL EV CA/RSA**

The following CAs co-form the hierarchical structure and were targets of the audit from May 18th 2017:

C. *I.CA SSL CA/RSA*

D. *I.CA Qualified CA/RSA*

E. *I.CA Qualified 2 CA/RSA*

F. *I.CA TSACA/RSA*

G. *I.CA Public CA/RSA*

Details of services are described below.

A. I.CA Root CA/RSA

The target of audit, the certification service **I.CA Root CA/RSA**, ETSI EN 319 411-1 policy EVCP *(other policies NCP, NCP+, DVCP, OVCP were target of the previous audit mentioned above)* and ETSI EN 319 411-2 policy QCP-w *(other policies - QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd were target of the previous audit mentioned above)*, and is described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = I.CA Root CA/RSA Certificate Serial Number: 05 f5 e1 00	
Name of CA (as in certificate)	serial number of certificate
CN = I.CA Root CA/RSA	05 f5 e1 00

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.6 as of 2017-11-20, I.CA

Certification Policy (CP):

"Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)", version 1.11 as of 2017-04-06, I.CA

B. I.CA SSL EV CA/RSA

The target of audit, the certification service **I.CA SSL EV CA/RSA 10/2017**, ETSI EN 319 411-1 policy EVCP and ETSI EN 319 411-2 policy QCP-w, is described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = I.CA Root CA/RSA Certificate Serial Number: 05 f5 e1 00	
Name of CA (as in certificate)	serial number of certificate
CN = I.CA SSL EV CA/RSA 10/2017	05 f5 e4 fe

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.6 as of 2017-11-20, I.CA

Certification Policy (CP):

"Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (algoritmus RSA)", version 1.00 as of 2017-11-16, I.CA

"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.11 as of 2017-11-20, I.CA

C. I.CA SSL CA/RSA

Certification service **I.CA SSL CA/RSA 07/2015**, ETSI EN 319 411-1 policies DVCP and OVCP, has been covered by the previous audit dated May 18th 2017.

D. I.CA Qualified CA/RSA

Certification service **I.CA Qualified CA/RSA 07/2015**, ETSI EN 319 411-2 policies QCP-n-qscd, QCP-l-qscd, has been covered by the previous audit dated May 18th 2017.

E. I.CA Qualified 2 CA/RSA

Certification service **I.CA Qualified 2 CA/RSA 02/2016**, ETSI EN 319 411-1 policies NCP, NCP+ and ETSI EN 319 411-2 policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, has been covered by the previous audit dated May 18th 2017.

F. I.CA TSACA/RSA

Certification service **I.CA TSACA/RSA 05/2017**, ETSI EN 319 411-2 policy QCP-l, has been covered by the previous audit dated May 18th 2017.

G. I.CA Public CA/RSA

Certification service **I.CA Public CA/RSA 07/2015**, ETSI EN 319 411-1 policies NCP, NCP+, has been covered by the previous audit dated May 18th 2017.

1.3.2 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", version 3.1 as of 2016-08-08, I.CA
Scope of the information security management system (ISMS):
"Rozsah ISMS", version 5.2 as of 2017-10-06, I.CA
Information security risk assessment and treatment:
"Analýza rizik - Důvěryhodné systémy pro vydávání certifikátů a časových razítek", version 1.0 as of 2017-03-13, I.CA
"Výběr protiopatření - Důvěryhodné systémy pro vydávání certifikátů a časových razítek", version 1.2 as of 2017-03-17, I.CA
"Zbytková rizika - Důvěryhodné systémy pro vydávání certifikátů a časových razítek", version 2.2 as of 2017-03-20, I.CA

1.4 Audit workflow

Schedule of audit:

Date	Activity
15.11.2017 – 21.11.2017	Stage 1 audit – verification of documentation I.CA Location: Office of Auditor (TAYLLOR & COX PCEB)
22.11.2017	Stage 2 audit – on site audit Location: Headquarter and operational premises of I.CA company
01.12.2017	Audit statement report, Qualifying Attestation Letter, Qualifying Attestation Cover Letter Location: Office of Auditor (TAYLLOR & COX PCEB)

Methodology:
ETSI EN 319 403 V2.2.2 (2015-08): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers"

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" part EV SSL certificates and qualified certificates for website authentication and "Information security risk analysis of its supporting trustworthy systems" 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 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 V1.1.1 (2016-02) 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 V2.1.1 (2016-02) 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: 2017-12-01

TAYLLORCOX s.r.o.
tayllorcox.com
Na Florenci 1055/35
110 00 Praha 1
010
IČO: 27902587 DIČ: CZ27902587