TAYLLOR & COX 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 319 411-2 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

and

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.

PART III: AUDIT INFORMATION

1.1 Audit scope

1.1.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM" ISSUING CERTIFICATES COMPLYING WITH:

1. ETSI EN 319 411-2 V2.1.1 (2016-02) policies:
    a) QCP-n Policy for EU qualified certificate issued to a natural person
    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
    c) QCP-l Policy for EU qualified certificate issued to a legal person
    d) 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

2. ETSI EN 319 411-1 V1.1.1 (2016-02) policies:
    a) NCP: Normalized Certificate Policy
    b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device
    c) DVCP: Domain Validation Certificate Policy
    d) OVCP: Organizational Validation Certificate Policy

The system consists of off-line root certification authority (I.CA Root CA/RSA) issuing certificates for CAs (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.

1.1.2 INFORMATION SECURITY RISK ANALYSIS:

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

1.2 Audit requirements

1.2.1 Certification services provided by 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 319 411-2 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 (policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd)
4. 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 (policies NCP, NCP+, OVCP, DVCP)
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 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
7. ETSI EN 319 412-3 V1.1.1 (2016-02)Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
8. ETSI EN 319 412-5 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
9. CEN/TS 419261 March 2015 Security requirements for trustworthy systems managing certificates and timestamps
10. ETSI TS 119 312 V1.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.2.2 I.CA's information security risk analysis

1. 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
2. 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
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 HIERARCHICAL STRUCTURE OF I.CA CA

A. Root CA/RSA

B. SSL CA/RSA

C. Qualified CA/RSA

D. Qualified 2 CA/RSA

E. TSACA/RSA

F. Public CA/RSA

Details of services are described below.

A. Root CA/RSA

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

Issuer of CA certificate (Root CA or intermediate 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 1.5 as of 2017-04-03, I.CA
Certification Policy (CP):
"Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)", version 1.11 as of 2017-04-06, I.CA

B. SSL CA/RSA

The target of audit, the certification service **I.CA SSL CA/RSA 07/2015**, ETSI EN 319 411-1 policies DVCP and OVCP, is described by the information contained in the certificate:

Issuer of CA certificate (Root CA or intermediate 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 CA/RSA 07/2015	05 f5 e4 ea

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.5 as of 2017-04-03, I.CA
Certification Policy (CP):
"Certifikační politika vydávání SSL certifikátů (algoritmus RSA)", version 1.10 as of 2016-03-29, I.CA
"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.10 as of 2015-11-02, I.CA

C. Qualified CA/RSA

The target of audit, the certification service **I.CA Qualified CA/RSA 07/2015**, ETSI EN 319 411-2 policies QCP-n-qscd, QCP-l-qscd, is described by the information contained in the certificate:

Issuer of CA certificate (Root CA or intermediate 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 Qualified CA/RSA 07/2015	05 f5 e4 ec

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice (algoritmus RSA)", version version 1.5 as of 2017-04-03, I.CA
Certification Policy (CP):
"Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA)", version 1.1 as of 2015-11-02, I.CA
"Certifikační politika vydávání kvalifikovaných certifikátů SK pro elektronické podpisy (algoritmus RSA)", version 1.10 as of 2017-03-13, I.CA
"Certifikační politika vydávání kvalifikovaných mandátních certifikátů SK (algoritmus RSA)", version 1.10 as of 2017-03-13, I.CA
"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě SK (algoritmus RSA)", version 1.10 as of 2017-03-13, I.CA
"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.10 as of 2015-11-02, I.CA

D. Qualified 2 CA/RSA

The target of audit, the certification service **I.CA Qualified 2 CA/RSA 02/2016**, ETSI EN 319 411-2 policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd and ETSI EN 319 411-1 policies NCP, NCP+, is described by the information contained in the certificate:

Issuer of CA certificate (Root CA or intermediate 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 Qualified 2 CA/RSA 02/2016	05 f5 e4 ee

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.5 as of 2017-04-03, I.CA
Certification Policies (CPs):
"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)", version 1.10 as of 2017-03-03, I.CA
"Certifikační politika vydávání systémových certifikátů (algoritmus RSA)", version 1.10 as of 2017-03-03, I.CA
"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (algoritmus RSA) (algoritmus RSA)", version 1.00 as of 2017-03-03, I.CA
"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.10 as of 2015-11-02, I.CA

E. TSACA/RSA

The target of audit, the certification service **I.CA TSACA/RSA 05/2017**, ETSI EN 319 411-2 policy QCP-l, is described by the information contained in the certificate:

Issuer of CA certificate (Root CA or intermediate 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 TSACA/RSA 05/2017	05 f5 e4 f4

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.5 as of 2017-04-03, I.CA
Certification Policies (CPs):
"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA)", version 2.00 as of 2017-04-03, I.CA
"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.10 as of 2015-11-02, I.CA

F. Public CA/RSA

The target of audit, the certification service **I.CA Public CA/RSA 07/2015**, ETSI EN 319 411-1 policies NCP, NCP+, is described by the information contained in the certificate:

Issuer of CA certificate (Root CA or intermediate 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 Public CA/RSA 07/2015	05 f5 e4 eb

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.5 as of 2017-04-03, I.CA
Certification Policy (CP):
"Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)", version 1.10 as of 2017-03-03, I.CA
"Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA)", version 1.10 as of 2017-03-03, I.CA
"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.10 as of 2015-11-02, I.CA

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 5.1 as of 2017-02-13, 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
13.04.2017 – 21.04.2017	Stage 1 audit – verification of documentation I.CA Location: Office of Auditor (TAYLLOR & COX PCEB)
09.05.2017 – 10.05.2017	Stage 2 audit – on site audit Location: Headquarter and operational premises of I.CA company
15.05.2017 – 18.05.2017	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" and "Information security risk analysis of its supporting trustworthy systems" was conducted in accordance with ETSI standards, in particular EN 319411-2, EN 319411-1, 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 319 411-2 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 and 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.

Part V: Signature and confirmation of audit report

Signature of lead auditor: Ing. Martin Dudek Praha: 2017-05-18	

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


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