

**TAYLLOR & COX s.r.o.**

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK  
Na Florenci 1055/35, Nové Město - Praha 1, CZ 110 00, info@tayllorcox.com  
TC SCEB - system certification board ISO/IEC 17021:11 accredited, TC SAIB service attest inspection board ISO/IEC 17020:12 accredited

**AUDIT STATEMENT REPORT – 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. (body accredited by Czech Accreditation Institute)**  
Na Florenci 1055/35  
Staré Město Praha 1  
CZ 110 00  
Czech Republic

Audit team: Ing. Radek Nedvěd  
Ing. Vít Lidinský, Ph.D.

**Part II: Conformity Evaluation of Service**

ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates", policies QCP public + SSCD, QCP public

and

ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates", policies NCP, NCP+, DVCP, OVCP

**TAYLLOR & COX s.r.o.**

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK  
Na Florenci 1055/35, Nové Město - Praha 1, CZ 110 00, info@tayllorcox.com  
TC SCEB - system certification board ISO/IEC 17021:11 accredited, TC SAIB service attest inspection board ISO/IEC 17020:12 accredited

## Part III: Audit information

### 1. Scope

"Hierarchical certificate issuing and management system" issuing qualified certificates complying with ETSI TS 101 456 policies QCP public + SSCD, QCP public and public key certificates complying with ETSI TS 102 042 certificate policies NCP, NCP+, DVCP, OVCP. 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 and I.CA Public CA/RSA), these CAs are issuing certificates for end users using registration authorities.

### 2. Audit target

Certification services provided by hierarchical structure of CAs: Root CA, SSL CA, Qualified CA, Qualified 2 CA, Public CA.

#### A. Root CA:

The target of audit, the certification service **I.CA Root CA/RSA**, ETSI TS 101 456 policies QCP public + SSCD, QCP public and ETSI TS 102 042 policies NCP, NCP+, DVCP, OVCP is described by the information contained in the certificate:

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

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice (algoritmus RSA)", version 1.3 as of 2016-04-06, I.CA

Certification Policy (CP):

"Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)", version 1.0 as of 2015-05-18, I.CA

#### B. SSL CA:

The target of audit, the certification service **I.CA SSL CA/RSA 07/2015**, ETSI TS 102 042 policies DVCP and OVCP, is described by the information contained in the certificate:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> CN = I.CA Root CA/RSA Certificate Serial Number: 05 f5 e1 00	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
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 1.3 as of 2016-04-06, 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

## TAYLLOR & COX s.r.o.

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK

Na Florenci 1055/35, Nové Město - Praha 1, CZ 110 00, info@tayllorcox.com

TC SCEB - system certification board ISO/IEC 17021:11 accredited, TC SAIB service attest inspection board ISO/IEC 17020:12 accredited



### C. Qualified CA:

The target of audit, the certification service **I.CA Qualified CA/RSA 07/2015**, ETSI TS 101 456 policies QCP public + SSCD, QCP public, is described by the information contained in the certificate:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = I.CA Root CA/RSA</b> <b>Certificate Serial Number: 05 f5 e1 00</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
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 1.3 as of 2016-04-06, 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 1.00 as of 2016-04-06, I.CA

"Certifikační politika vydávání kvalifikovaných mandátních certifikátů SK (algoritmus RSA)", version 1.00 as of 2016-04-06, I.CA

"Certifikační politika vydávání kvalifikovaných systémových certifikátů SK (algoritmus RSA)", version 1.00 as of 2016-04-06, I.CA

"Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)", version 1.10 as of 2015-11-02, I.CA

### D. Qualified 2 CA:

The target of audit, the certification service **I.CA Qualified 2 CA/RSA 02/2016**, ETSI TS 101 456 policies QCP public + SSCD, QCP public, is described by the information contained in the certificate:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = I.CA Root CA/RSA</b> <b>Certificate Serial Number: 05 f5 e1 00</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
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 1.3 as of 2016-04-06, I.CA

Certification Policies (CPs):

"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)", version 1.00 as of 2016-03-29, I.CA

"Certifikační politika vydávání systémových certifikátů (algoritmus RSA)", version 1.00 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

### E. Public CA:

The target of audit, the certification service **I.CA Public CA/RSA 07/2015**, ETSI TS 102 042 policies NCP and NCP+, is described by the information contained in the certificate:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = I.CA Root CA/RSA</b> <b>Certificate Serial Number: 05 f5 e1 00</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
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 1.3 as of 2016-04-06, I.CA

Certification Policy (CP):

"Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)", version 1.00 as of 2016-03-29, I.CA

"Certifikační politika vydávání komerčních certifikátů pro elektronické pečeti (algoritmus RSA)", version 1.00 as of 2016-03-29, I.CA

"Certifikační politika vydávání technologických (komerčních serverových) certifikátů (algoritmus RSA)", version 1.00 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

## TAYLLOR & COX s.r.o.

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK

Na Florenci 1055/35, Nové Město - Praha 1, CZ 110 00, info@tayllorcox.com

TC SCEB - system certification board ISO/IEC 17021:11 accredited, TC SAIB service attest inspection board ISO/IEC 17020:12 accredited

### 3. Audit requirements

ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates", policies QCP public + SSCD, QCP public and  
ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates", policies NCP, NCP+, DVCP, OVCP

### 4. Audit workflow

- A. Time period:  
from 2016-04-11 to 2016-05-18
- B. Location:  
Headquarter and operational premises of I.CA company
- C. Methodology:  
ETSI TS 119 403 V2.1.1 (2014-11): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers"
- D. Documentation and procedures:  
Policies and practices that rule the provision and operation of the certification services

### Part IV: Conclusion

Auditor confirms that the examination of I.CA's "Hierarchical certificate issuing and management system" was conducted in accordance with ETSI technical specifications, in particular TS 101 456, TS 102 042, TS 119 403 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**

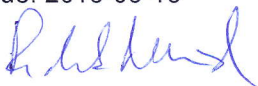
with requirements of ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates" and of ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

### Part V: Signatures and confirmation of audit report

Signature of lead auditor:

Ing. Radek Nedvěd

Prague: 2016-05-18



### TAYLLOR & COX s.r.o. TC SCEB

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK

Na Florenci 1055/35, Nové Město - Praha 1, CZ 110 00, info@tayllorcox.com

TC SCEB - system certification board ISO/IEC 17021:11 accredited, TC SAIB service attest inspection board ISO/IEC 17020:12 accredited