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 – POSTSIGNUM ROOT QCA

Part I: Basic information

Organization:	Česká pošta, s.p. (hereinafter PostSignum) Identification No.: 471 14 983 Politických vězňů 909/4, CZ 225 99 Praha 1, Czech Republic
Auditor:	TAYLLORCOX 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" ISSUING CERTIFICATES COMPLYING WITH

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

   a) NCP: Normalized Certificate Policy
   b) DVCP: Domain Validation Certificate Policy
   c) OVCP: Organizational Validation Certificate Policy

2) 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
   e) QCP-w Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person

The hierarchical structure of the system consists of off-line root certification authority (PostSignum Root QCA 2) issuing certificates for CAs these CAs (PostSignum Qualified CA 2, PostSignum Qualified CA 3, PostSignum Public CA 2, PostSignum Public CA 3) are issuing certificates for end users.

New root certification authority was started (PostSignum Root QCA 3) which didn´t issue any certificate yet.

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 PostSignum Root QCA as a part of hierarchical structure of PostSignum 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

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

1.2.2 PostSignum'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 27001:2013 Information technology Security techniques - Information security management systems – Requirements

1.3 Audit targets

1.3.1 CERTIFICATION SERVICES PROVIDED BY POSTSIGNUM CA

A. PostSignum Root QCA 2

B. PostSignum Root QCA 3

C. PostSignum Qualified CA 2

D. PostSignum Qualified CA 3

E. PostSignum Public CA 2

F. PostSignum Public CA 3

Details of services are described below.

A. PostSignum Root QCA 2

The target of audit, the certification service **PostSignum Root QCA 2**, ETSI EN 319 411-1 policies NCP, DVCP, OVCP and ETSI EN 319 411-2 policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QCP-w, and are described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = PostSignum Root QCA 2 Certificate Serial Number: 100	
Name of CA (as in certificate)	serial number of certificate (HEX / DEC)
CN = PostSignum Root QCA 2	64 / 100

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA v. 4.1", version 4.1 as of 08.09.2017.

Certification Policy (CP):

"Certifikační politika PostSignum Root QCA pro Kvalifikované systémové certifikáty podřízených CA v. 2.0", version 2.0 as of 03.01.2010.

B. PostSignum Root QCA 3

The target of audit, the certification service **PostSignum Root QCA 3**, ETSI EN 319 411-1 policies NCP, DVCP, OVCP and ETSI EN 319 411-2 policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QCP-w, and are described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = PostSignum Root QCA 3 Certificate Serial Number: 1000	
Name of CA (as in certificate)	serial number of certificate (HEX / DEC)
CN = PostSignum Root QCA 3	03e8 / 1000

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA v. 4.1", version 4.1 as of 08.09.2017.

Certification Policy (CP):

"Certifikační politika PostSignum Root QCA pro certifikáty podřízených CA v 1.0", version 1.0 as of 01.11.2017.

C. POSTSIGNUM QUALIFIED CA 2

The target of audit, the certification service **PostSignum Qualified CA 2**, ETSI EN 319 411-1 policy NCP, DVCP, OVCP and ETSI EN 319 411-2 policy QCP-n, QCP-n-qscd, QSP-l, QCP-l-qscd, QCP-w is described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = PostSignum Root QCA 2 Certificate Serial Number: 100	
Name of CA (as in certificate)	serial number of certificate (HEX / DEC)
CN = PostSignum Qualified CA 2	71 / 113

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA v. 4.1", version 4.1 as of 08.09.2017.

Certification Policies (CP):
"Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronický podpis v. 1.1", version 1.1 as of 08.09.2017.

"Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronickou pečeť v. 1.1", version 1.1 as of 08.09.2017.

"Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro autentizaci internetových stránek v. 1.0", version 1.0 as of 01.07.2017.

"Certifikační politika PostSignum Qualified CA pro certifikáty OCSP v. 3.0 21.06.2016", version 3.0 as of 21.06.2016.

D. POSTSIGNUM QUALIFIED CA 3

The target of audit, the certification service **PostSignum Qualified CA 3**, ETSI EN 319 411-1 policy NCP, DVCP, OVCP and ETSI EN 319 411-2 policy QCP-l, QCP-l-qscd, QCP-w is described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = PostSignum Root QCA 2 Certificate Serial Number: 100	
Name of CA (as in certificate)	serial number of certificate (HEX / DEC)
CN = PostSignum Qualified CA 3	A4 / 164

together with the:
Certification Practice Statement (CPS):
"Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA v. 4.1", version 4.1 as of 08.09.2017.

Certification Policies (CP):
"Politika vydávání časových razítek PostSignum TSA v. 1.1" , version 1.1 as of 08.09.2017.

E. POSTSIGNUM PUBLIC CA 2

The target of audit, the certification service **PostSignum Public CA 2**, ETSI EN 319 411-1 policy NCP is described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = PostSignum Root QCA 2 Certificate Serial Number: 100	
Name of CA (as in certificate)	serial number of certificate (HEX / DEC)
CN = PostSignum Public CA 2	72 / 114

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice pro úlohu Komerční certifikační autorita České pošty, s.p. PostSignum VCA v. 3.1", version 3.1 as of 01.02.2016.

Certification Policies (CP):

"Certifikační politika PostSignum Public CA pro komerční osobní certifikáty v. 3.0", version 1.1 as of 09.12.2013.

"Certifikační politika PostSignum Public CA pro komerční serverové certifikáty v. 3.1", version 3.1 as of 01.02.2016.

F. POSTSIGNUM PUBLIC CA 3

The target of audit, the certification service **PostSignum Public CA 3**, ETSI EN 319 411-1 policy NCP, DVCP, OVCP is described by the information contained in the certificate:

Issuer of CA certificate (Root CA): CN = PostSignum Root QCA 2 Certificate Serial Number: 100	
Name of CA (as in certificate)	serial number of certificate (HEX / DEC)
CN = PostSignum Public CA 3	C3 / 195

together with the:

Certification Practice Statement (CPS):

"Certifikační prováděcí směrnice pro úlohu Komerční certifikační autorita České pošty, s.p. PostSignum VCA v. 3.1", version 3.1 as of 01.02.2016.

Certification Policies (CP):

"Certifikační politika PostSignum Public CA pro komerční doménové certifikáty v. 3.0", version 3.0 as of 03.05.2017.

1.3.2 PostSignum's information security risk analysis

The target of audit, the PostSignum's Information security risk analysis of trustworthy systems supporting "Hierarchical certificate issuing and management system", is described by the information contained in the internal classified documentation of PostSignum.
PostSignum has implemented and certified quality and information security management systems in accordance with standards EN ISO 9001 and ISO/IEC 27001. Certification body for those managements are accredited certification body CQS.
Audit team made analyses in the Risk analyses report and from audit report of CQS issued 19.3.2017. Audit team not found any nonconformities, threats or discontinuities which could be make impact to working QTSP services.

1.4 Audit workflow

Schedule of audit:

Date	Activity
08.11.2017 – 14.11.2017	Stage 1 audit – verification of documentation PostSignum Location: Office of Auditor (TAYLLOR & COX PCEB)
21.12.2017	Stage 2 audit – on site audit Location: Headquarter and operational premises of PostSignum
21.12.2017	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 PostSignum'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 319411-1, 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.postsignum.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 Česká pošta, s.p.

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: 2017-12-21

MARTIN DUDEK

Datum: 2017.12.21 17:03:19 +01'00'