Správa základních registrů
Na Vápence 915/14
130 00 Praha 3

Praha 7. prosince 2018

NCA

CA PKI Disclosure Statement

Verze 1.0

CONTENTS

1 INTRODUCTION

This document gives basic information about the service provided by Správa základních registrů (hereinafter as SZR) of issuing qualified certificates including rights and duties of applicants.

This document gives only short selection of information which is fully contained in certification policies, in certification practice statements and in agreements with subscribers. It simplifies awareness of subscribers.

1.1 Document Evolution

Table 1 - Document Evolution

Version	Date of Release	Note
1.0	07.12.2018	First release.

1.2 SZR Audits and Inspections

Table 2 – Audits and Inspections

Type	Auditor/Inspector Statement
No audits and inspections were carried out so far.	

2 CONTACT INFORMATION

2.1 Head Office

The address of the head office:

Správa základních registrů

Na Vápence 14

130 00 Praha 3

Czech Republic.

Phone and mail contact to the head office:

tel.: +420 225 514 751

e-mail: epodatelna@szrcr.cz

2.2 Disclosure

All public information can be found on the Internet at http://www.szrcr.cz.

2.3 Communication with the Public

Communication with the public may be conducted as follows:

- general contact: epodatelna@szrcr.cz;
- registration authorities;
- technical support:
  - tel.: +420 225 514 758 (PO - PÁ 8:00 - 18:00ů
  - e-mail: podpora@szrcr.cz, the subject of the message must begin with text NCA;
- claims: podpora@szrcr.cz, the subject of the message must begin with text NCA.

3 CERTIFICATE TYPES, VERIFICATION PROCEDURES AND USE

3.1 Certificate Types

SZR issues certificates (for individuals and legal persons) which profile is compliant with standard X.509 v3.

The SZR root certification authority (RSA key length 3072 bits, algorithm SHA256) issues, in accordance with the requirements of technical standards and current legislation, certificates solely to subordinate CAs and to its OCSP responder.

The SZR subordinate certification authority SZR (RSA key length 3072 bits, algorithm SHA256) is intended for issuance of qualified certificates for electronic signature and qualified certificates for electronic seal to end users, for its OCSP responder and for issuance of infrastructure certificates.

End user certificates are issued in compliance with standards (and Czech technical standards, if applicable):

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 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.

3.2 Verification Procedures

In the process of issuing the initial certificate, when the physical presence of the applicant is necessary at the registration authority office (with exceptions as indicated in the following paragraph), the identity of this individual is always verified on the basis of his/her personal papers. In the case of a certificate for an organization, the certificate applicant's relationship with the organization is verified.

If the relevant certification policy allows issuance of a “subsequent certificate” (a certificate that will comply with the agreement on the provision of relevant services, concluded between

the applicant and SZR, issued to the applicant on the basis of a new application for a certificate during the validity period of the certificate for which this subsequent certificate is issued), then the physical presence of the applicant for a certificate at the registration authority office is not required. A detailed description of registration procedures is provided in the relevant certification policies.

4 USE OF CERTIFICATES

Qualified certificates may be used in compliance with 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

Other types of certificates may generally be used to verify electronic signatures, for identification, authentication, and for secure communication.

When using certificates, it is always necessary to proceed in accordance with the applicable certification policy.

Unless the relevant legislative standard specifies otherwise, audit records and records generated during the registration process are kept for at least 10 years from their inception.

SZR retains issued certificates and lists of revoked certificates for the entire period of its existence.

5 OBLIGATIONS OF APPLICANTS AND SUBSCRIBERS

A subscriber is the applicant for a certificate to whom/which this certificate was issued. From the point of view of SZR this is the natural person or legal entity who/which entered into subscriber agreement with SZR. The basic obligations of the applicant for this certificate, and subsequently the subscriber, include:

- to provide truthful and complete information when registering the application for issuance of the certificate;
- to inform immediately the certification service provider of changes in data contained in the issued certificate, respectively in the agreement;
- to familiarize himself/herself with the certification policy under which the certificate was issued;
- to check whether the information given in the application for the certificate and in the certificate itself are correct and match the required data;
- to use the devices and the private key corresponding to the public key in the issued certificate in such a way so as to prevent its unauthorized use;
- to use the private key and the corresponding issued certificate in accordance with the relevant certification policy and solely for the purposes set out in this certification policy;
- to immediately request revocation of the certificate and terminate the use of the relevant private key, especially in the case of private key compromise or suspicion that the private key has been abused.

6 OBLIGATIONS OF THE RELYING PARTIES

Relying parties are entities who, in their work, rely on the certificate issued by SZR. The basic obligations of these entities include;

- to obtain, from a secure source, relevant certificates of certification authorities as referred to in Chapter 3.1, and to verify the checksum of these certificates;
- before using the end-user certificate, to verify the validity of CA certificates relating to the certificate of the end user;
- to make sure that the end-user certificate is suitable for its use;
- to comply with all relevant provisions of the certification policy under which the end-user certificate was issued.

7 LIMITATIONS OF WARRANTY AND RESPONSIBILITY

SZR:

- undertakes to fulfill all of the obligations as defined both by applicable laws and regulations, and by relevant certification policies;
- shall provide the above guarantees for the duration of the agreement on the provision of certification services; if a breach of obligations on the part of the subscriber or the relying party having a connection with the alleged damage is determined, the warranty claims shall not be provided – this must be reported to the subscriber or to the relying party and recorded;
- does not provide any guarantees other than those mentioned above;
- other possible damages based on the provisions of relevant laws, and their amounts, may be decided upon by the court.

SZR is not liable:

- for defects of provided services incurred due to improper or unauthorized use of services, particularly for operating in violation of the conditions specified in the certification policy, as well as for defects caused by force majeure, including temporary loss of telecommunication connection, etc.;
- for damages resulting from the use of the certificate in the period after requesting its revocation, if SZR complies with the defined deadline for publishing the revoked certificate on the certificate revocation list (CRL).

8 AGREEMENT AND CERTIFICATION POLICY

The relationship between the subscriber and SZR apart from the relevant provisions of mandatory legislation is governed by the agreement and by the relevant provisions of applicable certification policies.

The relationship between the relying party and SZR is governed by the relevant provisions of the applicable certification policies. The relationship between SZR and the relying parties is not governed by agreement.

All public information can be obtained from the contact addresses listed in Chapter 2 of this document.

9 PERSONAL DATA PROTECTION

The protection of personal data at SZR is resolved in compliance with applicable legislation concerning personal data, i.e. Czech Republic Act no. 101/2000 Coll. on Personal Data Protection, as amended and REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

10 REFUND POLICY AND CLAIMS

A claim may be submitted as follows:

- by e-mail to podpora@szrcr.cz, the subject of the message must begin with text NCA;
- by registered mail to the address of the SZR head office;
- by sending a message to the SZR data mailbox;
- in person at the SZR head office.

The claiming person (subscriber) must provide:

- a description of the defects and their manifestations, as accurately as possible;
- the serial number of the claimed product;
- requested way of handling the claim.

SZR will decide upon the complaint within three working days from receipt of the complaint and will notify the claimant (by e-mail or registered mail), unless the parties agree otherwise.

Complaints, including defects, will be processed without undue delay and not later than thirty days from the date of claim, unless the parties agree otherwise.

The holder shall be provided with a new certificate in the following cases:

- if there is reasonable suspicion that the private key of the certification authority was compromised;
- if the specific certification authority, when receiving the request for issuance of a certificate, discovers that there exists a different certificate with a duplicate public key.

11 LEGAL ENVIRONMENT

The activities of SZR are governed by the relevant current provisions of the legislation, in particular:

- by REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- by Czech Republic Act No. 297/2016 Coll., on trust services for electronic transaction;
- by Czech Republic Act No. 90/2012 Coll., on business corporations;
- by Czech Republic Act No. 101/2000 Coll., on the protection of personal data and the amendments of certain laws;
- by REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

12 QUALIFICATION, AUDITS, INSPECTIONS

SZR is a qualified provider of trust services. The provision of these services is regularly subjected to audits and inspections according to the legislation requirements mentioned above in the Chapter 11.

On behalf of Správa základních registrů

Ing. Michal Pešek