NFQES CA Certification Policy

Version: **2.5**

Effective date: 1.5.2024

PO-01

Policy

Public

Created by:

Ing. Martin Berzák
Security Manager

28.3.2024

Approved:

Ing. Eduard Baraniak
Managing Director brainit.sk, s. r. o.

28.3.2024

brainit.sk, s. r. o.

Veľký Diel 3323, 010 08 Žilina
ID: 52577465

www.brainit.sk

History of changes

Version	Date	Authors	Description	Reason for changes
1.0	1.4.2020	Ing. Martin Berzák	First approved version of the document	
2.0	1.12.2020	Ing. Eduard Baraniak	Revised version of the document according to RFC3647	
2.1	15.2.2021	Ing. Martin Berzák	Incorporated comments of the NSA	
2.2	15.3.2021	Ing. Martin Berzák	Modified Chapters 3.2.2 with 3.2.3	
2.3	15.3.2022	Ing. Martin Berzák Bc. Paula Höhrová	Modified chapters 1.3.3, 1.6, 3.2.2, 3.2.3, 3.3, 4.1.1, 4.1.2, 4.9.1, 4.9.2, 9.1.1, 9.4.1, 9.12.2	Extension to Mandate Certificate and Registration Authorities
2.4	1.3.2023	Ing. Martin Berzák	Modified Chapters 3.2.2 and 3.2.3	Extension to the possibility of authentication of the identity of FOs and POs without the need for KEP
2.5	2.3.2023	Ing. Martin Berzák	Modified chapters 4.1.4, 4.5.1, 6.4.1	Extension to enable authorization using the NFQES Qualified Authenticator mobile app - OCRA software token
2.5	27.3.2024	Ing. Michal Šterbák, PhD.	Modified Chapter 6.9	Adoption of previous TCs and extension of the long-term retention functionality with the ability to store entire files and their hashes. -

TABLE OF CONTENTS

1 Introduction 10
1.1 Overview 10
1.2 Title and identification of the document 11
1.3 PKI participants 11
1.3.1 Certification authorities 11
1.3.2 Registration authorities 11
1.3.3 Users, Customer, or Participants 11
1.3.4 Relying parties 12
1.3.5 Other participants 12
1.4 Use of the certificate 13
1.4.1 Appropriate use of the certificate 13
1.4.2 Prohibited use of the certificate 13
1.5 Policy administration 13
1.5.1 Information about the provider and contact details 13
1.5.2 Contact person 14
1.5.3 The person who determines the suitability of the CPS for the certification policy 14
1.5.4 CPS approval procedures 14
1.6 Definitions and abbreviations 14
2 Disclosure and responsibility for data storage 16
*2.1 Repositories ..... **Chyba! Záložka nie je definovaná.***
2.2 Disclosure of certification authority information 16
2.3 Time or frequency of publication 16
2.4 Access controls to repositories 16
3 Identification and authentication 17
3.1 Naming 17
3.1.1 Types of names 17
3.1.2 The need for meaningfulness of names 17
3.1.3 Anonymity or pseudo-anonymity of subscribers 17
3.1.4 Rules for interpreting different forms of names 17
3.1.5 Uniqueness of names 17
3.1.6 Recognition, authentication and the role of trademarks 17
3.2 Initial identity verification 17
3.2.1 Method of proving ownership of the private key 18
3.2.2 Legal entity identity authentication 18
3.2.3 Authentication of the identity of a natural person 19
3.2.4 Device or system identity authentication 20
3.2.5 Unverified information on the applicant 21
3.2.6 Validation of authority 21
3.2.7 Interoperability criteria 21

3.3 Identification and authentication for key rekey requests *21*
3.4 Identification and authentication for the revocation request *21*
4 Operational requirements for the certificate life cycle **22**
4.1 Application for a certificate *22*
4.1.1 Who can apply for a certificate 22
4.1.2 Registration process and responsibilities 22
4.1.3 Generating a request 23
4.1.4 Sending a certificate application 23
4.2 Processing the application for a certificate *23*
4.2.1 Performing identification and authentication functions 23
4.2.2 Approval or rejection of certificate applications 23
4.2.3 Time for processing certificate applications 24
4.3 Issuance of the certificate *24*
4.3.1 CA actions during certificate issuance 24
4.3.2 Notification by the CA to the applicant of the issuance of a certificate 24
4.4 Receipt of the certificate *24*
4.4.1 Behaviour that constitutes acceptance of a certificate 24
4.4.2 Publication of the certificate. 24
4.4.3 Notification of the issuance of a CA certificate to other entities 24
4.5 Using public keys and certificates *25*
4.5.1 Using a subscriber's private key and certificate 25
4.5.2 Use of a public key and relying party certificate 25
4.6 Renewal of certificate *25*
4.7 Issuance of a subsequent certificate *26*
4.7.1 Conditions for the issue of a subsequent certificate 26
4.7.2 Who can apply for a subsequent certificate 26
4.7.3 Processing requests for the issuance of a subsequent certificate 26
4.7.4 Notification of the issue of a subsequent certificate 26
4.7.5 Behaviour that constitutes acceptance of a subsequent certificate 26
4.7.6 Publication of the subsequent certificate 26
4.7.7 Notification of the issue of a subsequent certificate to other entities 26
4.8 Modifying the certificate *26*
4.9 Certificate revocation *26*
4.9.1 Conditions for certificate revocation 26
4.9.2 Who can apply for certificate revocation 27
4.9.3 Procedure for requesting the revocation of a certificate 27
4.9.4 Time limit for submitting an application for cancellation of the QC 28
4.9.5 Time within which the CA must process the cancellation request 28
4.9.6 Cancellation control requirement for relying parties 28
4.9.7 Frequency of issuing CRLs 28

4.9.8 Maximum latency for CRL 29
4.9.9 Availability of OCSP service 29
4.9.10 OCSP control requirements 29
4.9.11 Other forms of availability of certificate revocation information 29
4.9.12 Special requirements for changing keys after they have been compromised 29
4.9.13 Circumstances in which the QC is suspended 29
4.9.14 Who can apply for suspension of QC 29
4.10 Services related to certificate status 29
4.10.1 Operational requirements 29
4.10.2 Service availability 29
4.11 End of service provision 30
5 Physical, personnel and operational security measures 31
5.1 Physical security 31
5.1.1 Premises 31
5.1.2 Physical access 31
5.1.3 Power supply and air conditioning 31
5.1.4 Protection from water 31
5.1.5 Fire prevention and protection 32
5.1.6 Media storage 32
5.1.7 Waste disposal 32
5.1.8 Backup off the main site 32
5.2 Procedural precautions 32
5.2.1 Trusted roles 32
5.2.2 Number of persons required for the task 32
5.2.3 Identification and authentication for each role 32
5.2.4 Roles requiring division of responsibilities 32
5.3 Personnel security measures 32
5.3.1 Qualification, experience and vetting requirements 32
5.3.2 Verification requirements 33
5.3.3 Requirements for training 33
5.3.4 Training renewal frequency 33
5.3.5 Roll rotation frequency 33
5.3.6 Penalties for unauthorised conduct 33
5.3.7 Requirements for external suppliers 33
5.3.8 Documentation provided by the employee 33
5.4 Procedures for obtaining audit records 33
5.4.1 Types of recorded events 34
5.4.2 Frequency of processing of audit records 34
5.4.3 Retention period of the audit report 34
5.4.4 Audit log protection 34

5.4.5 Audit log backup procedures 34
5.4.6 Audit collection system (internal vs. external) 34
5.4.7 Notification of the entity initiating the audit 34
5.4.8 Vulnerability assessment 34
5.5 Archive of records 34
5.5.1 Types of archived records 34
5.5.2 Retention period for the archive 35
5.5.3 Archive protection 35
5.5.4 Archive backup procedures 35
5.5.5 Time stamp requirements for records 35
5.5.6 Archiving system 35
5.5.7 Procedures for obtaining and verifying archival information 35
5.6 Change the key 35
5.7 Recovering from compromise and disaster 35
5.7.1 Procedures for dealing with compromise and disasters 35
5.7.2 Computing resources, software or data are corrupted 36
5.7.3 Private key compromise procedures 36
5.7.4 Maintaining business continuity after a disaster 36
5.8 Termination of CA or RA 36
6 Technical safety measures 38
6.1 Generating and installing a key pair 38
6.1.1 Generating key pairs 38
6.1.2 Delivery of the private key to the subscriber 38
6.1.3 Delivery of the public key to the certificate issuer 38
6.1.4 Delivery of the CA public key to relying parties 38
6.1.5 Key sizes 38
6.1.6 Public parameter generation and quality control 38
6.1.7 Key Uses (by X.509 v3 key use field) 39
6.2 Private key protection and cryptographic module design 39
6.2.1 Cryptographic module standards and controls 39
6.2.2 Private key (n of m), multi-person control 39
6.2.3 Saving the private key 39
6.2.4 Private key backup 39
6.2.5 Private key archive 39
6.2.6 Private key transfer to or from the cryptographic module 39
6.2.7 Storing the private key on the cryptographic module 39
6.2.8 How to activate the private key 39
6.2.9 How to deactivate the private key 40
6.2.10 Method of destroying the private key 40
6.2.11 Cryptographic module evaluation 40

6.3 Other aspects of key pair management ... 40
6.3.1 Public Key Archive ... 40
6.3.2 Certificate operating periods and key pair usage periods ... 40
6.4 Activation data ... 40
6.4.1 Generating and installing activation data ... 40
6.4.2 Activation of data protection ... 40
6.4.3 Other aspects of activation data ... 41
6.5 Computer security checks ... 41
6.5.1 Specific technical requirements for computer security ... 41
6.5.2 Computer security assessment ... 41
6.6 Life cycle measures ... 41
6.6.1 System development checks ... 41
6.6.2 Safety management controls ... 41
6.6.3 Life cycle safety measures ... 41
6.7 Network security controls ... 42
6.8 Time stamp ... 42
6.9 Qualified electronic signature/seal storage service ... 42
7 Certificate, CRL and Processes OCSP ... 44
7.1 Certificate Profile ... 44
7.1.1 Version numbers ... 44
7.1.2 Certificate parameters ... 44
7.1.3 Certificate Extension ... 44
7.1.4 Algorithm object identifiers ... 46
7.1.5 Forms of names ... 46
7.1.6 Restrictions on names ... 46
7.1.7 Certification policy identifier ... 46
7.1.8 Using extensions to restrict the policy ... 46
7.1.9 Syntax and semantics of politics ... 46
7.1.10 Extension ... 46
7.2 Profile of CRL ... 46
7.2.1 Version numbers ... 46
7.2.2 CRL and CRL input extensions ... 47
7.3 Profile of OCSP ... 47
7.3.1 Version numbers ... 47
7.3.2 OCSP Extensions ... 47
8 Compliance audit and other assessments ... 47
8.1 Frequency or circumstances of assessment ... 47
8.2 Identity/qualifications of the assessor ... 47
8.3 Relationship of the evaluator to the evaluated entity ... 48
8.4 Topics covered by the evaluation ... 48

8.5 Measures taken as a result of the shortfall *48*
8.6 Announcement of results *48*
9 Other business and legal matters **49**
9.1 Fees *49*
9.1.1 Fees for the issue or renewal of a certificate 49
9.1.2 Fees for access to the certificate 49
9.1.3 Fees for appeal or access to status information 49
9.1.4 Charges for other services 49
9.1.5 Refund Policy 49
9.2 Financial responsibility *49*
9.2.1 Insurance cover 49
9.2.2 Other assets 49
9.2.3 Insurance or guarantee for end-users 49
9.3 Confidentiality of business information *50*
9.3.1 Scope of confidential information 50
9.3.2 Information which does not fall within the scope of confidential information 50
9.3.3 Responsibility for the protection of confidential information 50
9.4 Privacy Policy *51*
9.4.1 Data Protection Plan 51
9.4.2 Information considered private 51
9.4.3 Information that is not considered private 51
9.4.4 Responsibility for the protection of private information 51
9.4.5 Notification and consent to the use of private information 51
9.5 Intellectual property rights *51*
9.6 Declarations and warranties *52*
9.6.1 CA representations and warranties 52
9.6.2 RA Declaration and Warranties 52
9.6.3 Declarations and warranties of participants 52
9.6.4 Representations and warranties of the relying parties 53
9.6.5 Representations and warranties of other participants 53
9.7 Disclaimer of warranties *53*
9.8 Limitations of liability *53*
9.9 Compensation *54*
9.10 Duration and termination *54*
9.10.1 Deadline 54
9.10.2 End 54
9.10.3 Termination and survival effect 54
9.11 Individual notifications and communication with participants *54*
9.12 Amendments *54*
9.12.1 Amendment procedure 54

9.12.2 Mechanism and notification period 55
9.12.3 Circumstances in which the OID must be changed 55
9.13 Dispute resolution provisions 55
9.14 Applicable law 55
9.15 Compliance with applicable legislation 56
9.16 Miscellaneous provisions 56
10 Links 57

1 Introduction

Certification Policy for certificates of certification keys of the NFQES Certification Authority (hereinafter referred to as "CP"), presents the binding procedures, methodology, and responsibilities of the company brainit.sk s. r. o., ID No.: 52577465 registered in the Commercial Register of the District Court of Žilina, Section: Sro, Insert No. 72902/L (hereinafter referred to as "Provider") for the issuance and management of certificates of certification keys of the Certification Authority (hereinafter referred to as "CA").

The CP is a binding document, serving as a standard of practices, procedures, and principles to be followed by all parties involved.

The provider's website is at https://nfqes.sk

In the event of a difference between the Slovak and English versions of the Certification Policies and Certification Policy Statements, the provisions set out in the Slovak version shall apply.

1.1 Overview

The structure of the CP is in accordance with RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". The CP is used for products and services provided by the Provider and for the management of certificates according to the X.509 standard in the implementation of the Public Key Infrastructure (hereinafter referred to as "PKI").

This CP covers the provision of the following qualified trust services:

- **Qualified trusted service for issuing and verifying qualified certificates for electronic signature, where the private key is stored in a qualified electronic signature/seal creation device (QSCD)**
  (OID 0.4.0.194112.1.2)
- **Qualified trusted service for issuing and verifying qualified certificates for an electronic seal, where the private key is stored in a qualified electronic signature/seal creation device (QCSD)**
  (OID 0.4.0.194112.1.3)
- **Qualified trust service for the production and verification of qualified certificates for the authentication of websites**
  (OID 0.4.0.194112.1.4)
- **Qualified trust service for storing qualified electronic signatures**
- **Qualified trust service for storing qualified electronic seals**

Provider's certification authorities for the provision of qualified trust services:

Provider's Certification Authority	Certificate serial number	Publisher
CA NFQES	01	self-signed

CP applies equally to all certificates issued for the Provider's needs, namely:

- Certification Authority Certificate
- Certificate to validate the existence and validity of the certificate (OCSP)
- Intermediate Certification Authority

1.2 Title and identification of the document

Document version: 2.5

Effective date: 1.5.2024

The CP for NFQES CA certification key certificates is identified by the object identifier OID 1.3.158. 52577465 .0.0.0.0.1.3.2, where the individual components of the OID have the following meanings:

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** unique identifier of the company brainit.sk s.r.o. (IČO)
- **0.0.0.1** CA NFQES
- **3** Document "NFQES CA Certification Policy"
- **2** major version of the document

1.3 PKI participants

This chapter describes the identity or types of entities that perform the roles of participants within the PKI.

1.3.1 Certification authorities

Certification Authority:

- is an entity that provides the qualified trust services referred to in Chapter 1.1,
- is part of the hierarchical PKI structure in the issued qualified certificates (QC issuer)

The Provider's certification authorities are:

- CA NFQES (serial number: 01), which issues qualified certificates to users and is not part of any hierarchical PKI structure (Self-signed certificate).

1.3.2 Registration authorities

A Registration Authority (hereinafter referred to as "RA") is an entity that acts on behalf of the Provider, performing selected activities in the provision of the Provider's trust services in accordance with this CP as amended from time to time.

The Provider has established an internal RA which is intended for all interested parties who are interested in the qualified trust services referred to in Chapter 1.1. This RA is not a separate legal entity.

1.3.3 Users, Customer, or Participants

Customer means a legal entity or a natural person to whom the Provider provides Trust Services based on the agreed Contract and this person also pays for the services.

The holder of a Qualified Certificate (QC) is the person named in the QC. The Certificate Holder may be one person - the Customer, or two different persons in case the Customer is an employer, but the Certificate Holder is an employee. In case of an electronic signature, the certificate holder is the signatory.

The Certificate Holder may be:

- natural person,
- a natural person identified in connection with a legal entity,
- a legal entity, which may be an organization or a unit or department thereof,

- a facility or system operated by or on behalf of a natural person or legal entity.

If the Customer is a natural person and only his/her first and last name are listed as the subject, then the Customer and the Holder of the QC are the same natural person, i.e. in the event of non-fulfilment of the obligations imposed on both the Customer and the Holder, this natural person is directly liable.

When the Customer acts on behalf of one or more Holders with which it is connected (e.g. the Customer is a legal entity requesting the issuance of QC for its employees), the different responsibilities of the Customer and the Holder are defined in the document GTC for the Provision and Use of the Trusted Certificate Issuance and Verification Service" published on the Provider's website.

https://nfqes.sk/dokumenty/

The conditions to be fulfilled by the Certificate Holder and the Customer are defined in this CP.

The relationship between the Customer and the Holder may be as follows:

When applying for a QC of a natural person (Holder), the Customer is

- the natural person himself,
- a legal entity authorized to represent a natural person (Holder), or
- any entity with which the natural person (Holder) is associated.

When applying for a QC for a legal entity, the Customer is

- any entity which is authorized under the relevant legal system to represent a legal entity; or
- the statutory body of the legal entity applying on behalf of its subsidiaries or units or divisions.

When applying for a QC for a facility or system operated by an individual or legal entity, the Customer is:

- the natural person or legal entity operating the installation or system,
- the statutory body of the legal entity applying on behalf of its subsidiaries or units or divisions.

1.3.4 Relying parties

Relying parties are natural person or legal entity who rely on the trusted services of the Provider for their actions.

1.3.5 Other participants

Policy Management Authority

The Policy Management Authority (PMA) is a component of the Provider established for the purpose of:

- overseeing the creation and updating of the CPs, including the evaluation of changes and plans for the implementation of any changes adopted,
- review audit results to determine whether the Provider is responsibly complying with the provisions of the issued CPS,
- guidance and management of the Provider's activities as well as the RA,
- interpretation of the provisions issued by the CPS and its instructions to the Provider and the RA,
- review of the CPS to ensure that the Provider's practice complies with the relevant CP,
- making recommendations to the Provider regarding corrective and other appropriate action,
- the performance of the function of internal auditor, entrusting this activity to an independent employee.

The PMA represents the top-level decision maker in all matters and aspects relating to the Provider and its activities.

Other service providers

Other service providers include:

- OCSP responder Provider that provides QC validation services.

1.4 Use of the certificate

A QC made for a natural person where the private key is in the QSCD (policy identifier 1.3.158.36061701.0.0.0.0.1.2.2 [QCP-n-qscd]) is made for the purpose of supporting a qualified electronic signature within the meaning of Article 3 (12) of the eIDAS Regulation.

A QC made for a legal entity where the private key is in the QSCD (policy identifier 1.3.158.36061701.0.0.0.0.1.2.2 [QCP-l-qscd]) is made for the purpose of supporting a qualified electronic seal within the meaning of Article 3 (27) of the eIDAS Regulation.

The QC produced for web site authentication (policy identifier 1.3.158.36061701.0.0.0.0.1.2.2 [QCP-w]) is produced for the purpose of supporting web site authentication within the meaning of Article 3 (38) and Article 45 of the eIDAS Regulation.

1.4.1 Appropriate use of the certificate

No provisions

1.4.2 Prohibited use of the certificate

No provisions

1.5 Policy administration

1.5.1 Information about the provider and contact details

Name: brainit.sk, s. r. o.

Headquarters: Veľký Diel 3323, 010 08 Žilina

IČO: 52577465

DIČ: 2121068763

IČ DPH: SK2121068763

Register: the Commercial Register of the District Court of Žilina, section Sro, insert number 72902/L

Contact:

Mobile: +421 918 022 030

E-mail: info@brainit.sk

Provider's website: https://nfqes.sk/

Trust Services website: https://zone.nfqes.sk/

Supervisory authority:

Contact for Certificate cancellation request:

Mobile: +421 918 022 030

E-mail: info@nfqes.sk

1.5.2 Contact person

For policy creation, the Provider has established a Policy Management Authority (PMA) (see point 1.3.5), which is fully responsible for its content, and which is ready to answer all questions concerning the Provider's policies.

Certification Authority CA NFQES:

Address Veľký Diel 3323, 010 08 Žilina

Email: ca@nfqes.sk

Phone: +421 905 320 821

Website: https://nfqes.sk

To report incidents: infra@nfqes.sk

1.5.3 The person who determines the suitability of the CPS for the certification policy

The person responsible for deciding whether the Provider's procedures set out in the CA CP or CA CPS comply with this Policy is the PMA (see clause 1.3.5).

1.5.4 CPS approval procedures

The Provider should have its CP and CPS approved prior to commencement of operations and must meet all its requirements. The content of the CP and CPS shall be approved by the person appointed to the PMA role.

Once approved by the PMA, the relevant document is published in accordance with the Publication and Notification Policy.

The PMA is to communicate its decisions in such a way that this information is readily accessible to parties relying on the QC.

1.6 Definitions and abbreviations

Certificate:

- a certificate or a qualified certificate for electronic signature within the meaning of the eIDAS Regulation,
- a certificate or a qualified certificate for an electronic seal within the meaning of the eIDAS Regulation,
- certificate for authentication of the website in accordance with the eIDAS Regulation.
- mandate certificate within the meaning of Act No. 272/2016 Coll. on trust services,
- any other certificate used for encryption, authentication or other purposes as defined in the Provider's Policy, which has been or is to be issued by the Provider to the Customer.

CRL – Certificate Revocation List - a list of Certificates cancelled before their expiry date.

Trust Services - qualified trust services for the issuance and verification of Certificates provided by the Provider in accordance with the eIDAS Regulation, the Act, and the Provider's Policies. Trust Services may also be composed of other associated services in connection with Certificates.

These are mainly:

- Certificate Verification - providing information on the validity or revocation of Certificates - CRL, OCSP response,
- generation of key pairs,
- and more...

Certificate Holder - the person named in the Certificate who is the holder of the private key associated with the public key to which the Certificate is issued.

Regulation eIDAS - Regulation No 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/ES.

OCSP Response - A response to an OCSP request that gives an indication of the validity of the Certificate at the specified time.

OCRA token - a hardware token that conforms to the RFC6287 standard - OCRA: OATH Challenge-Response Algorithm

Provider Policy/ies -

- the policy of the Trust Service Provider for issuing and verifying qualified certificates, which applies to qualified certificates issued by the Provider under the eIDAS Regulation,
- policy for the provision of trusted service for the issuance and verification of qualified certificates, covering other Certificates not listed in the above clause.

The Provider's policies include all regulations and their updates issued by the Provider and published on its website.

Provider - company brainit.sk, s. r. o. with registered office Veľký diel 3323, Žilina 010 08, IČO: 52577465, registered in the Commercial Register of the District Court of Žilina, Section Sro, insert number. 72902/L.

Acknowledgement - an acknowledgement of receipt of a Certificate by which the Certificate Holder acknowledges, among other things, receipt of the Certificates.

Department - the place where Certificates are issued. It is a place operated by the Provider - its registered office.

Relying Party - a natural person or legal entity who relies on the Provider's Trusted Services to act.

General Terms and Conditions (abbreviated as "GTC") - this document defines the General Terms and Conditions for the provision and use of the trusted service for the issuance and verification of certificates, always in their effective version.

Qualified device - a device for making an electronic signature/seal that meets the requirements set out in Annex II to the eIDAS Regulation.

Contract - Contract for the provision of trusted service of issuing certificates concluded between the Provider and the Customer, or any other contract between the Provider and the Customer, the subject of which is the provision of Trust Services.

Contract with CA - a contract concluded between the Provider and the Certificate Holder, regulating the rights and obligations of the parties to the use of the Certificate.

Customer - means a natural person or legal entity to whom the Provider provides Trust Services based on the agreed Contract and the person who pays for these services.

2 Disclosure and responsibility for data storage

2.1 Storage

The storage sites must be located to be accessible to the QC Holders and the Cooperating Parties and in accordance with the overall security requirements.

The website will serve as the provider's storage site. The exact URL is set out in Chapter 1. The Provider's website is publicly accessible via the internet to QC Holders, relying parties and the public.

Publicly available information listed on the Provider's website and is of a controlled access nature.

2.2 Disclosure of certification authority information

The Provider must publish, in an online mode, a repository that is accessible to Customers, QC Holders and Relying Parties that will contain, at a minimum, the following information:

- the current CRL as well as all CRLs issued since the start of the QC drawing activity,
- Provider's own CA certificates, which belong to its public keys, whose corresponding private key is used for signing the executed QCs and CRLs.

The Provider must publish this CP as well as other documents related to the provision of trust services under this CP in an online mode via its website.

2.3 Time or frequency of publication

A list of revoked certificates (CRL) shall be published as specified in Chapter 4.9.7. Information about the revoked CRL shall be available on the Provider's website (see Chapter 1), which serves as its storage.

CPs and CPSs or revisions thereof shall be published as soon as possible after their approval and issue.

All other information to be published in the repository must be published as soon as possible.

2.4 Access controls to storage

The Provider must protect all information stored in the repository that is not intended for public dissemination. The provider must make every effort to ensure the confidentiality, integrity and availability of the data resulting from the trust services provided. It must also take logical and security measures to prevent unauthorized access to the repository by persons who could in any way damage, alter, amend, or delete the data stored in the storage.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

Each CA shall be able to generate certificates that contain X.500 Distinguished Names [10], specifically in accordance with X.501 [11] and X.520 [12] respectively, and names in the sense of the RFC5322 Internet Message Format [13].

Customers must choose for themselves the distinguished name to be included in their QC.

3.1.2 The need for meaningfulness of names

The term "meaningfulness" means that the form of the name takes a commonly used form to establish the identity of the Holder (natural person, legal entity, public authority, website)

The names used must reliably identify the person to whom they are assigned.

In some cases, accented characters are not used in the content of the QC and are replaced by equivalent characters from the ASCII character table (e.g., “á” is replaced by “a”; “č” is replaced by “c”, etc.). This may be requested by the customer if the equipment on which the QC is to be used is a dedicated HW that cannot be replaced (or is unprofitable for the customer) and does not support the UTF-8 character set.

3.1.3 Anonymity or pseudo-anonymity of subscribers

The Provider does not support the issuance of a QC with a pseudonym and the Provider may not issue a QC to an anonymous Holder.

3.1.4 Rules for interpreting different forms of names

The interpretation of the various forms of names in the QCs produced by the Provider shall be in accordance with the QC profiles described in Chapter 7 of this CP.

3.1.5 Uniqueness of names

The provider is responsible for the clarity of names throughout the QC holder community.

3.1.6 Recognition, authentication, and the role of trademarks

The Provider does not guarantee to any entity that its name in the QC will contain its trademark, even at its express request.

Only trademarks whose ownership or lease has been satisfactorily documented by the customer may be used in QC. No other authentication of the provider's trademarks shall be performed.

A Provider shall not knowingly issue Qualified Certificates containing a name that has been determined by a court of competent jurisdiction to infringe another entity's trademark. Provider is not obligated to examine trademarks or resolve trademark disputes.

3.2 Initial identity verification

This section contains a description of the identification and authentication procedures related to each entity (Customer, Holder, CA, RA, or other Participant).

In case of declaration of an emergency situation on the territory of the Slovak Republic within the meaning of Act No. 42/1994 Coll. on Civil Protection of the Population, the PMA may decide to modify the method of issuance of QC stored in the QSCD and the related generation of cryptographic key pairs and authentication of the identity of individual entities, which will be different from the procedures

set out in this document. The modified procedure, which will be adapted to the conditions of the emergency and therefore cannot be further specified, must be in writing, must be approved by the PMA, must be assessed by the Conformity Assessment Body, must not contravene Regulation (EU) No 910/2014 and national legislation, and may only be used for the duration of the emergency. After the end of the emergency, the procedures set out here must be followed.

3.2.1 Method of proving ownership of the private key

A key pair for which a QC for an electronic signature intended for the execution of a qualified electronic signature or a QC for an electronic seal intended for the execution of a qualified electronic seal must be generated directly in a qualified electronic signature or seal execution facility that meets the requirements set out in Annex II of the eIDAS Regulation [3], known as QSCD.

All QC requests for site authentication where the key pair is not stored in a QSCD must be in PQCS#10 format, which means that the QC request will be signed with the private key belonging to the public key contained in that QC request.

Under no circumstances shall any component of the Provider archive private keys belonging to the holder of a QC issued by the Provider. The only exceptions are private keys managed by the Provider for third parties in the context of the provision of a data management service for the execution of an electronic signature or an electronic seal on behalf of the signatory (issuer) (see Annex II of the eIDAS Regulation).

3.2.2 Legal entity identity authentication

Verification of the identity of the legal entity can be carried out at the RA's registered office and remotely at any location by signing the application for issuance using the certificates for the qualified electronic signature of all the managing directors, which are stored in the electronic ID card with chip (eID) issued in accordance with Article 24(a) or (b) of the eIDAS Regulation. The list of managing directors is obtained from the electronic extract from the commercial register valid for legal transactions, which the Client must provide, for example, via the slovensko.sk portal. Subsequently, all signatures are verified, thereby verifying the validity of the signatures, the validity and authenticity of the data and the validity of the identification documents. The RA employee then checks whether the data provided in the AdES signatures and in the certified electronic extract from the Commercial Register match the data provided in the zone.nfqes.sk application and in the application for the issuance of the certificate. If the certificates are valid, the electronic extract from the commercial register is valid and the data in the application, the certificate application, the extract from the commercial register and the data in the AdES signature match, the legal entity is verified.

Verification of the identity of a legal entity may also be carried out at the RA headquarters or outside the RA headquarters in the presence of a responsible employee of the RA (customer visit) in the physical presence of the statutory body authorized to act on behalf of the company, also with the use of at least two valid identity documents for each member of the statutory body, of which at least one document of each member of the statutory body must be an official document with the likeness of the face, the so-called face-to-face identification. In this case, the statutory body shall bring a commercial register extract valid for legal transactions not older than 3 months, the statutory body authorized to act on behalf of the company shall personally sign and agree the GTC and the statutory body authorized to act on behalf of the company shall sign the application for a certificate. The RA officer will assess the validity and authenticity of the identification documents (checking the various security features of the documents) and retain copies of the documents submitted. If the RA officer finds anything questionable in the documents, he must reject them. He or she will then check whether the data from the extract from the commercial register applicable for legal transactions and the data on the identification documents match the data provided in the application at zone.nfqes.sk and in the

application for a certificate. If the data provided in the application and in the application for the certificate match the data on the identification documents and in the extract from the commercial register, the legal entity shall be deemed to be verified.

Identification documents of a member of the statutory body must contain at least:

- name and surname,
- permanent address,
- birth number or date of birth.

In the case of non-business entities such as a civic association, municipality, church, foundation, etc., in addition to its identity, such legal entity must also demonstrate the legality or "reason" for its existence, using and referring to the law or other regulation dealing with that type of entity, the charter of incorporation, etc.

3.2.3 Authentication of the identity of a natural person

Verification of a natural person's identity can be carried out at the RA's registered office and remotely at any location by means of a certificate for a qualified electronic signature stored in an electronic ID card with a chip (eID) issued in accordance with Article 24(a) or (b) of the eIDAS Regulation, with which the natural person signs and agrees to the GTC and the natural person signs the application for the issue of the certificate. In both cases (at the RA's premises and remotely), this qualified signature is verified, thereby verifying the validity of the signature, the validity and authenticity of the data and the validity of the identification documents. The RA employee then checks whether the data provided in the AdES signature matches the data provided in the zone.nfqes.sk application and in the certificate application. If the certificate is valid and the data in the application, the certificate application, and the data in the AdES signature match, the individual is authenticated.

Verification of the identity of a natural person may also be carried out at the RA headquarters or outside the RA headquarters in the presence of a responsible RA employee (customer visit) in the physical presence of the person, also with the use of at least two valid identity documents, at least one of which must be an official document with a facial image, the so-called face-to-face identification. In this case, the individual shall personally sign and agree to the GTC, and the individual shall sign the application for the certificate. The RA officer will assess the validity and authenticity of the identity documents (checking the various security features of the documents) and keep copies of these submitted documents. If the RA officer finds anything questionable on the documents, he/she must reject them. He/she will then check that the information on the identification documents matches the information given in the application on zone.nfqes.sk and in the application for the certificate. If the data in the application and in the certificate application match the data in the identification documents, the natural person shall be deemed to be authenticated.

Identification documents of a natural person must contain at least:

- name and surname,
- permanent address,
- birth number or date of birth.

If a natural person represents another natural person, he or she must additionally prove that he or she has been authorized by the authorizing natural person to act on his or her behalf in the matter in question, by means of an officially certified power of attorney.

In the case of a mandate certificate within the meaning of Section 8 of Act No. 272/2016 Coll., which relates to acting on behalf of another person or a public authority, the Customer must submit an authorization to act on behalf of the represented person in the form of:

- a document proving that the person concerned is a statutory body of the legal entity or public authority concerned,
- the credentials, if the natural person is an employee of the legal entity on whose behalf he or she acts and is in an employment or similar employment relationship with that legal entity,
- a power of attorney certified by a notary public if the natural person concerned is not in an employment or similar employment relationship with the person concerned.

In the case of a mandate certificate within the meaning of Section 8 of Act No. 272/2016 Coll., which relates to the performance of an activity or the performance of a function, the Customer must credibly demonstrate that it is a public authority, that it performs the activity or function in accordance with the requirements of Act No. 272/2016 Coll. and in accordance with the requirements specified in the list of authorizations for the given authorization, which is published on the NBÚ web site.

3.2.4 Device or system identity authentication

The provider must also guarantee, even if the QC is made for the purpose of authenticating the website, that the identity of the website and its public key are linked accordingly.

For this reason, the quality control of a website must be formally assigned to a person acting on behalf of a legal entity (organization) that has demonstrable control over the website for which the quality control is being carried out. All the conditions set out in chapters 3.2.2 and 3.2.3 apply, as well as the other conditions set out in this chapter.

The natural person is obliged to provide the Provider with the following information:

- system/device public keys (contained in the QC application),
- identification of the system/device,
- the authorizations of the system/device and its attributes (if any to be specified in the QC),
- contact details so that the Provider can communicate with that person if necessary.

The provider must verify and authenticate the correctness of aby authorization (item value with a distinguished name) to be included in the QC and will verify the data submitted.

The methods for carrying out this process and data verification shall include:

- verification of the identity of the natural person in accordance with the requirements of point 3.2.3,
- or verification of the identity of the legal entity to which the component belongs, in accordance with the requirements of point 3.2.2,
- verification of the eligibility of the use of the data to be included in the individual QC entries, with emphasis on the content of the commonName entry.

Note: The typical value of this entry is the fully qualified domain name (FQDN).

In the case of the use of a domain name, it is a condition that the relevant second and higher-level domain is under the control of the Customer requesting the issue of a QC for website authentication.

Verification that the Customer is the owner of the domain or has control over the domain whose FQDN is or will be listed in the Subject Alternative Name (SAN) item of the CN request must be done in one of the following ways:

- By sending a randomly generated value via email to the email address identified as the authorized contact for the domain in the registry of the authorized registrar for the domain (e.g. for the .sk domain it is whois.sk-nic.sk). The randomly generated value must be sent along with the confirmation of the TLS/SSL certificate request eligibility in a return email message

from the email address to which it was sent. The random value shall be unique for each email message sent. If the validation of the eligibility to use the FQDN is successful in this way, the Provider may issue other TLS/SSL certificates that end with the same FQDN. This method can also be used to validate a request to issue a wildcard QC for website authentication.

- By telephone, by calling the number identified as the authorized contact for the domain in the registry of the authorized registrar for the domain (e.g. for the .sk domain it is whois.sk-nic.sk) and verifying the legitimacy of the request for the issuance of a TLS/SSL certificate by the Customer.

If it cannot be reliably established by any of the described methods that the Customer has the domain under legitimate control, the Provider must refuse to issue a QC for the request.

The CMA must ensure that the QC subject:organizationUnitName (OU) item is carefully checked so that it does not contain a legal entity name, trademark, trade name, address, location, or other text pointing to an identifiable natural person or legal entity without verifying this information.

Checking details on documents

An electronic document signed with a qualified electronic signature/seal:

- validity of the qualified electronic signature,
- the identity of the signatory (principal, registrar of companies, statutory body, etc.).

3.2.5 Unverified information on the applicant

All items in a qualified certificate must be verified.

3.2.6 Validation of authority

See point 3.2.3

3.2.7 Interoperability criteria

The Provider does not apply any interoperability criteria.

3.3 Identification and authentication for key rekey requests

Issuing a subsequent QC means changing the QC key pair - a new QC will be created, which will have the same distinguished name as the original, but the new QC will have a different public key (corresponding to the new, different private key), a different Serial Number, and may have a changed validity length.

A customer applying for a subsequent QC must comply with the requirements of the original registration (in particular, verification of their identity).

Issuance of a subsequent mandate certificate or remotely without the personal presence of the holder or a person authorized by him/her is not possible.

Upon cancellation of a QC, the Holder must comply with the identification requirements of the initial registration when making a subsequent QC.

3.4 Identification and authentication for the revocation request

The request to revoke of QC must be verified, see paragraph 4.9.

A request for revocation of a QC may be verified using the private key belonging to the QC to be revoked, regardless of whether the private key has been compromised or not.

4 Operational requirements for the certificate life cycle

4.1 Application for a certificate

4.1.1 Who can apply for a certificate

The provider may request the issue of:

- QC for electronic signature
  - a natural person or a natural person authorized by the Holder or a person acting on behalf of the Holder on the basis of the law or a decision of a competent authority
- QC for electronic seal
  - any entity (the Customer) which, under applicable national legislation, has the authority to act on behalf of the legal entity in question
- QC for website authentication
  - the natural person or legal entity operating the installation or system
- mandate certificate
  - a natural person authorized by law or by virtue of the law to act for or on behalf of another person or a public authority or a natural person who performs an activity pursuant to a special regulation (§8 (1) of Act No. 272/2016 Coll.) or performs a function pursuant to a special regulation (§8 (1) of Act No. 272/2016 Coll.).
  - any entity (Customer) with which the individual is associated, e.g. his/her employer, a non-profit organization of which he/she is a member, etc.

4.1.2 Registration process and responsibilities

The Customer must take the following steps in preparation for the Provider's visit:

- to familiarize themselves with the GTC for the provision and use of the trusted service of issuing and verifying certificates brainit.sk, s.r.o. and the Information on the processing of personal data, which must be available in a readable form through a permanent communication channel (see zone.nfqes.sk),
- Familiarize yourself with the procedure and, where appropriate, the principles and guidelines for obtaining QC,
- prepare the values of the individual items of the QC request so that these values are consistent with this CP,
- prepare your chosen identity documents or other necessary documents,
- in the case of a mandate certificate, prepare an authorization to act on behalf of the represented person (declaration, a power of attorney or notarially certified power of attorney or documents proving that he or she is a public authority or that he or she is a public authority), according to the list of authorizations published on the NBÚ website.
- in case of registration by RA to arrange a date for the visit.

Procedure prior to the issue of the QC

Prior to issuing the QC, the employee representing the Provider must:

- inform the individual present about the GTC,
- verify the identity of the Holder/Customer or the person who represents him/her according to the submitted documents and record all mandatory personal data in the information system (IS) of the Provider,
- verify all other documents submitted according to the established procedures.

4.1.3 Generating a request

In case of QC for website authentication, the Provider's employee must check the received QC request in PQCS#10 format before verifying the Customer's identity. The content of the application items and the obligation to complete them shall be checked.

In the case of key pair generation directly at the Provider, the confidentiality of the data generated in this way must be ensured.

The Provider must always verify that the device on which the keys are generated, whether directly at the Provider or under the control of the Customer, is QSCD certified.

For security reasons, a QC request or the public key contained therein for which a QC has already been issued cannot be reused to issue another QC and must be rejected by the RA.

4.1.4 Sending a certificate application

If the QC is made on a QSCD device, the RA must forward the request directly to the QSCD device for processing via the zone.nfqes.sk application. The entire zone.nfqes.sk application is accessible to the RA worker only after authorization using the name, password, and the associated OCRA token or the activated NFQES Qualified Authenticator software OCRA token, and the validation of the request and subsequent processing of the request in the QSCD device is also confirmed by the RA worker's enforced authorization. Once the request is processed in the zone.nfqes.sk application, all authorizations are then transferred to the person for whom the QC is being issued, while all provisions of Chapter 6.4 are complied with.

Requests for the issuance of a certificate for the authentication of a website where cryptographic keys are not stored in the QSCD shall be sent by the Customer to the RA, which shall perform all procedures related to the certificate generation process.

4.2 Processing the application for a certificate

4.2.1 Performing identification and authentication functions

Identification and authentication of the Holder of each type of QC shall be carried out in accordance with clauses 3.2.2 and 3.2.3 when the subsequent certificate is issued in accordance with clause 3.3.

Once the authentication and identification of the QC Holder has been carried out and the required personal data has been entered into the Provider's IS, the RA must carry out the data entry of the QC application and, in the case of the use of a pre-sent electronic application, carry out a visual check of the application.

The check of data completion (personal data and data in the application for QC) will also be carried out by the application used by the RA worker (zone.nfqes.sk), which will not allow to continue with the QC in case of an incomplete item, which is mandatory or in case of an incorrectly completed item.

4.2.2 Approval or rejection of certificate applications

The Provider shall not issue a QC until all verifications and any changes, if necessary, have been completed.

If the Certificate Holder's key pair was not generated directly by the provider, an automated check must be performed to verify that the public key contained in the request matches the private key used to sign the request.

The Provider is fully responsible for the verification of the Holder's/Customer's data.

The provider has the right not to create a QC, even if the customer has successfully passed the registration process with the provider, if a serious fact is subsequently detected that prevents the issuance of a QC (e.g. an error in the application format).

In the event that for some reason a QC cannot be issued for a given application, the RA must inform the customer of this fact.

The Provider must inform the Holder of the issue of the QC in an appropriate manner.

4.2.3 Time for processing certificate applications

Once the request is sent to the Provider's system, the QC should be issued to the Customer as soon as possible.

4.3 Issuance of the certificate

4.3.1 CA actions during certificate issuance

Once a request for a QC has been sent from the internal RA to the Provider's system, the Provider must perform a verification of the received request to verify that:

- has been sent to authorized RA staff,
- conforms to the PQCS#10 standard.

The issuance of a qualified certificate on a key pair generated directly in the RA is securely bound to this generation procedure.

If all requirements for the issue of the QC are met, the Provider must issue the QC.

Once the QC has been issued a QSCD, the Provider must ensure the QC's exclusive control over its private key.

During the lifetime of the issuing CA, its distinguished name shall not be transferred to another entity.

At the Customer's request, the Provider may make a QC in the production environment to verify and test its functionality. In such a certificate, it must be clearly stated in the distinguished name items that it is a test certificate. All requirements of this CP relating to verification of the identity of the QC Holder must be met in the execution of such QC.

4.3.2 Notification by the CA to the applicant of the issuance of a certificate

The Provider must inform the Holder of the issue of the QC in an appropriate manner.

4.4 Receipt of the certificate

4.4.1 Behaviour that constitutes acceptance of a certificate

The Provider must securely hand over the issued certificate to its Holder.

4.4.2 Publication of the certificate.

QCs that contain the personal data of the Holder may not be disclosed to the public to protect the personal data of their Holders.

4.4.3 Notification of the issuance of a CA certificate to other entities

The Provider must inform the National Security Authority about the issuance of a QC in accordance with the requirements of Section 6 (2) of Act No. 272/2016 Coll.

4.5 Using public keys and certificates

This section describes the responsibilities related to the use of keys and certificates.

4.5.1 Using a subscriber's private key and certificate

The QC Holder's obligation in relation to the private key and the QC is:

- provide the Provider with true, accurate and complete information in accordance with this CP when applying for a certificate,
- use the key pair in accordance with the restrictions set out in the GTC,
- always protect his private keys in accordance with this CP, the GTC, so that they are under his sole control,
- use the private key only after receiving QC to the public key with which it forms a pair,
- in the case of a QC that has not yet expired, immediately notify the Provider if it suspects that:
    - their private key has been lost, stolen, or compromised,
    - lost control of the private key by compromising his or her login credentials (password or OCRA token or mobile phone with an active NFQES Qualified Authenticator application - software OCRA token),
    - inaccuracies or changes in the content of the certificate,
    - immediately request the cancellation of the QC in the event that any of the information provided in the QC entity has become invalid,
- refrain from using a private key and QC that has expired, been revoked, or compromised (including if the Provider itself has been compromised and the Holder/Customer is aware of it),
- comply with all terms, conditions and restrictions imposed on the use of your private key and QC, such as discontinuing the use of your private key upon expiration or revocation of the QC public key,
- to use the QC provided only for the relevant purposes,
- immediately stop using the private key once it has been compromised,

The obligations of the QC Holder also apply to the natural person or legal entity that has taken over the certificates for the components or websites it manages.

4.5.2 Use of a public key and relying party certificate

The relying parties are obliged to:

- use the QC only for the purpose for which it was issued,
- verify each QC for validity (i.e., verify that the QC is currently valid and is not on the provider's current CRL) before relying on the QC,
- establish a trust relationship with the CA that issued the QC by verifying the certification path in accordance with the X.509 version 3 standard and the mandatory use of the trusted list of the country in which the issuer resides, as specified in the countryName entry of the issuer's name in the qualified certificate,
- store the original signed data, the applications necessary to read and process that data, and the cryptographic applications necessary to verify the qualified electronic signatures of that data, insofar as it may be necessary to verify the signature of that data.

4.6 Renewal of certificate

The provider shall not issue a QC on a public key on which it has already issued a QC in the past.

4.7 Issuance of a subsequent certificate

The term subsequent certificate means the issuance of a new QC of the same type and with the same content for an existing Holder whose personal data are entered in the Provider's system.

4.7.1 Conditions for the issue of a subsequent certificate

No provisions.

4.7.2 Who can apply for a subsequent certificate

Additional QC may be requested by an existing Holder to whom the Provider has previously issued a QC and who meets the identification and authentication requirements of clause 3.2.

4.7.3 Processing requests for the issuance of a subsequent certificate

A subsequent QC must be issued in the same manner as the original QC was issued.

4.7.4 Notification of the issue of a subsequent certificate

The Provider must inform the Holder in an appropriate manner of the issuance of the subsequent QC.

4.7.5 Behaviour that constitutes acceptance of a subsequent certificate

See paragraph 4.4

4.7.6 Publication of the subsequent certificate

See paragraph 4.4.2.

4.7.7 Notification of the issue of a subsequent certificate to other entities

No provisions

4.8 Modifying the certificate

The Provider does not support the issuance of a new QC without a change to the key pair due to changes related to its content.

4.9 Certificate revocation

4.9.1 Conditions for certificate revocation

The QC must be revoked when the binding between the Holder and its public key in the certificate is no longer considered valid. The Provider is obliged to revoke the QC it manages in the following cases:

- the Certificate Holder applies for revocation of the certificate,
- finds that the requirements of the eIDAS Regulation or Act No. 272/2016 Coll. have not been met when issuing the QC,
- the court shall order the Provider to dissolve the CC by its decision,
- finds that the QC has been issued based on false information,
- learns that the QC Holder has died if it is a natural person or has ceased to exist if it is a legal entity,
- discovers that a private key belonging to the QC has been compromised, e.g. if access to a private key belonging to a public key listed in the QC is known to a person other than the Holder listed in the QC,
- the Holder has breached its obligations under this CP and/or the GTC,
- it becomes aware that the information on the certificate has become outdated,

- becomes aware that the Holder has become incapacitated by a court order,
- the Provider's private key has been compromised.

In the case of a mandated certificate, it shall request revocation:

- mandator,
- mandatary,
- a public authority or a person with whom the mandator performs an activity pursuant to a special regulation (§8 (1) of Act No. 272/2016 Coll.) or performs a function pursuant to a special regulation (§8 (1) of Act No. 272/2016 Coll.)

4.9.2 Who can apply for certificate revocation

The Holder of a QC (or a natural person or legal entity authorized by it) may at any time request, in the manner set out in this CP, the cancellation of its own QC, without having to state the reason for the request for cancellation.

He may also request the revocation of his certificate:

- the Provider - the employee in question is obliged to document this fact, including the reason for his/her action,
- an entity (natural person or legal entity) based on the inheritance procedure (the Provider must attach to the documents on the dissolution of the QC a copy of the documents from which the right of the entity to apply for the dissolution of the QC is derived),
- the court through its judgment or interim measure (the Provider must attach a copy of the relevant court decision to the documents on the cancellation of the QC),
- a person authorized by the court, e.g. the guardian of the QC entity to be dissolved (the Provider must attach a copy of the relevant court decision to the documents on the dissolution of the QC).
- a public authority or a person with whom the mandator has performed an activity pursuant to a special regulation (§8 (1) of Act No. 272/2016 Coll.) or a function pursuant to a special regulation (§8 (1) of Act No. 272/2016 Coll.), the mandator or the mandatary, respectively.

4.9.3 Procedure for requesting the revocation of a certificate

The authorized person must apply for revocation of the qualified certificate in person to the provider. The person requesting revocation of the QC must complete the same authentication process with the Provider as required for the initial registration of the Holder/Customer (see paragraph 3.2), or provide an agreed password for revocation of the QC, which will be provided to the Holder/Customer upon issuance of the Qualified Certificate.

To prevent arbitrary revocation of a QC by an unauthorized party, authentication of the QC revocation request is important.

The holder/customer of the QR may be represented by an authorised person with the Provider in connection with the revocation of the QR. The representative person must submit a certified power of attorney or power of attorney, the text of which clearly expresses the will of the Holder/Client to cancel the QR.

The Provider may refuse a revocation QC request if the Holder/Customer fails to authenticate their identity.

The RA must check the validity of the certificate to be revoked. If it is a certificate that is no longer valid, the RA must refuse the request for revocation as it is not possible to revoke a certificate that has expired or been revoked.

In the event of a legitimate request for cancellation of a QC and successful verification of the identity of the Holder/Customer, the QC must be cancelled as soon as possible (see clause 4.9.5).

The holder of a valid QC may also request revocation of his/her QC by sending a request by e-mail to the Provider's contact e-mail address specified in point 1.5.2, which shall contain a message with an unambiguously expressed wish to cancel the QC, namely the sentence "I hereby request cancellation of the qualified certificate with the serial number "----*sn*----", with the revocation password being: "----*abcde*----", where the Customer fills in the real data valid for the QC he/she is requesting to revoke.

A request for certificate revocation may also be made in writing. The Certificate Holder/Customer must specify in the written request the serial number of the QC whose revocation is requested and must authenticate the revocation using a valid revocation password for that QC.

The Provider must inform the QC Holder of the cancellation of the QC upon cancellation.

4.9.4 Time limit for submitting an application for cancellation of the QC

In the event of a threat of compromise of the private key, the authorized person (see 4.9.2) must submit a request for revocation of the QC as soon as possible. In person, revocation can only be requested during the working hours determined by the internal RA, whose working hours are published on the Provider's website (see paragraph 1). If the request is made electronically, it can be sent to the internal RA at any time.

4.9.5 Time within which the CA must process the cancellation request

The provider must:

- revoke the QC no later than 24 hours after verification of the facts that the request for revocation of the certificate in question is justified,
- Publish the current list of revoked QCs and any previous lists of revoked certificates so that they are accessible to Customers/Holders and all relying parties,
- inform the Customer/QC Holder of the revocation of his/her QC by sending an e-mail to the e-mail address provided by the Holder during the RA registration process, including the reason for the revocation of the QC in question,
- archive all CRLs it has issued,
- synchronize the system time used as the source for the certificate revocation time with UTC time at least every 24 hours.

The CRL must be published to the repository as soon as possible after its release.

4.9.6 Cancellation control requirement for relying parties

The relying party is obliged to verify the validity of the QC by relying on the available CRL or OCSP.

In the time between the submission of a legitimate request for revocation of a QC and the publication of the revoked QC in the CRL, the Certificate Holder/Customer bears all responsibility for any damage caused by the misuse of his/her QC. After the certificate is published in the CRL, the party that relied on the revoked QC shall bear all liability for any damages caused using the revoked QC.

Failure to verify the validity of a QC using a CRL or OCSP shall be considered a gross violation of this CP.

4.9.7 Frequency of issuing CRLs

The requirements for the frequency of issuing a Certificate Revocation List (CRL) are as follows:

Publisher CRL	**Frequency of issue**	**nextUpdate thisUpdate interval**
CA NFQES	12 hours	24 hours

4.9.8 Maximum latency for CRL

The Provider must ensure that the time from the issuance of the CRL to its publication in the repository does not exceed 120 seconds.

4.9.9 Availability of OCSP service

The URIs of the OSCP responder addresses of the Provider's individual issuing CAs must be included in the Authority Information Access certificate extension. In accordance with the eIDAS Regulation, the OCSP service must be provided free of charge.

4.9.10 OCSP control requirements

Third parties wishing to use the OCSP service must send a request to the appropriate OCSP responder whose URI is published in the QC whose validity they wish to verify. The request sent shall comply with the requirements of RFC 6960.

4.9.11 Other forms of availability of certificate revocation information

Verification of the current certificate status can be done manually by:

- lists of current CRLs, as well as an archive of all issued CRLs for individual CA of the Provider, available at:
  - https://zone.nfqes.sk/crl/
- the Provider must ensure that a telephone or e-mail enquiry regarding the status of a particular certificate is answered.

4.9.12 Special requirements for changing keys after they have been compromised

No provisions.

4.9.13 Circumstances in which the QC is suspended

Pursuant to Section 7(2) of Act No. 272/2016 Coll. on Trust Services, a qualified trust service provider to which the Authority has granted a qualified status may not temporarily suspend the validity of a QC for an electronic signature or a QC for an electronic seal.

4.9.14 Who can apply for suspension of QC

No provisions.

4.10 Services related to certificate status

4.10.1 Operational requirements

The list of revoked certificates (CRL) shall be available at the URL specified in clause 4.9.11 and shall be accessible via HTTP protocol on port 80.

The OCSP service shall be available at the URL address specified in the issued qualified certificate and the requestor shall send a request for the status of the certificate in accordance with clause 4.9.10.

4.10.2 Service availability

Service availability is 24/7 at SLA level 99%

4.11 End of service provision

If the holder/customer decides to terminate the contractual relationship with the provider before the expiry of the validity period of the issued QC, he/she must at the same time apply for revocation of the certificate.

5 Physical, personnel and operational security measures

The security of the provider must be based on a set of security measures in the areas of object, personnel, physical and operational security. These security measures must be designed, documented, and applied based on security rules. These measures must be approved by the Provider's management.

Safety precautions must be available to all relevant personnel.

The provider must:

- take full responsibility for ensuring that its activities comply with the procedures defined in its security policy,
- have a list of all its assets indicating their classification in the light of the risk assessment carried out.

The Provider's security policy and asset summary relating to security must be reviewed at regular intervals.

The Provider's security policy and summary of security-related assets must be reviewed when significant changes are made to ensure their continuity, appropriateness, sufficiency, and effectiveness.

All changes that may affect the level of security provided must be approved by the Provider's management.

The Provider's systems setup must be periodically reviewed for changes that compromise the Provider's security policy.

5.1 Physical security

5.1.1 Premises

The technological premises in which the Provider's basic infrastructure is located must be in protected areas that are accessible only to authorized persons. These areas must be separated from other areas by appropriate security features (security doors, grilles, solid walls, etc.). The Provider's facilities shall consist only of equipment intended for the provision of trust services and qualified trust services and shall not be used for any purpose unrelated to those services.

5.1.2 Physical access

The access control mechanisms to the Provider's protected premises, i.e. to the premises of the highest security zone, must be secured in such a way that these premises must be protected by a security alarm and access to them may be allowed only to persons who possess a security token and are listed on the list of persons authorized to enter the Provider's protected premises. The Provider's equipment must be always protected against unauthorized access, including unauthorized physical access. Any entry of other persons must be always recorded and may only be permitted when accompanied by an authorized person.

5.1.3 Power supply and air conditioning

The premises in which the Provider's equipment is housed shall be adequately supplied with electricity and air-conditioned to create a reliable operating environment.

5.1.4 Protection from water

The premises in which the Provider's equipment is located shall be so located that they cannot be endangered by water from any source. Where this is not entirely possible, measures must be taken to minimize the risk of the premises being exposed to water.

5.1.5 Fire prevention and protection

The premises in which the Provider's equipment is located must be reliably protected from sources of direct fire, ice or heat that could cause a fire on the premises.

5.1.6 Media storage

Media should be stored in areas that are protected from accidental, unintentional damage (water, fire, ice, electromagnetic). Media containing security audit, archive or back-up information is to be stored in a location separate from the Provider's equipment.

5.1.7 Waste disposal

Waste arising in connection with the Provider's operations must be handled in such a way that the environment is not polluted in any way.

5.1.8 Backup off the main site

In the event of irreversible damage to the premises of the main site where the Provider's infrastructure is located, it is necessary to have at least copies of the Provider's critical assets backed up outside the main site.

5.2 Procedural precautions

5.2.1 Trusted roles

The provider must have defined trusted roles responsible for different aspects of the trust services provided (e.g. system administrator, security manager, internal auditor, policy manager, etc.) that form the basis of trust in the entire PKI.

At the same time, the responsibilities of each role must be defined.

Persons selected to fill roles that require credibility must be trustworthy and accountable.

All persons in trusted roles must be free of conflicts of interest to ensure the impartiality of the services provided by the Provider.

5.2.2 Number of persons required for the task

For each task, the number of individuals who are designated to perform each task must be identified (the K of N rule).

5.2.3 Identification and authentication for each role

Each role must have a defined method of authentication and identification when accessing the Provider's IS.

5.2.4 Roles requiring division of responsibilities

Each role must have set criteria that consider the need for separation of functions in terms of the role itself i.e. roles that cannot be performed by the same individuals must be listed.

5.3 Personnel security measures

Provider personnel must be formally appointed to trusted roles by the executive management responsible for security.

5.3.1 Qualification, experience, and vetting requirements

Staff in positions of trust must meet the qualification and experience requirements and should have a security clearance of a specified level.

Persons in managerial positions must:

- have relevant experience or training in the trust services provided by the Provider,
- be familiar with the security measures for roles responsible for security,
- have experience in information security and risk assessment to the extent necessary for the performance of the management function.

5.3.2 Verification requirements

It is recommended that an employee to be placed in a trusted role have a security clearance of a specified level or be in the process of applying for this type of clearance. Personnel security measures are ensured by the Provider's internal mechanisms.

5.3.3 Requirements for training

For some trusted roles, there may be some specific training requirements that you should complete before or during placement. Topics should include operation of CMA software and hardware, security and operational procedures, provisions of this CPS, CP, etc.

5.3.4 Training renewal frequency

For tasks requiring prescribed training, the need for refresher training after primary training may be established.

5.3.5 Roll rotation frequency

No provisions.

5.3.6 Penalties for unauthorized conduct

Failure by any employee of the Provider to comply with the provisions of this CP or the adopted CPS, whether in bad faith or through negligence, shall be subject to appropriate disciplinary and administrative action, which may result in termination of employment or civil or criminal penalties.

Any inappropriate or unauthorized conduct by an employee in a position of trust that is discovered by the provider's management shall result in immediate removal from the position of trust pending completion of the pending management review. After management review and mutual discussion or review of the results of the investigation with the employee, the employee may be dismissed from employment or reassigned to a trusted role, as appropriate.

5.3.7 Requirements for external suppliers

Independent contractors who may be entrusted with trusted tasks shall be subject to the same obligations and specific requirements for those tasks under the provisions of clause 5.3 and shall also be subject to the sanctions set out in clause 5.3.6.

5.3.8 Documentation provided by the employee

Employees in positions of trust must have the documents necessary to perform the function for which they are entrusted, including a copy of this CP or CPS and all technical and operational documents necessary to maintain the integrity of the provider's operations. This information must also include security and internal system documentation, authentication procedures and policies, as well as other information prepared by the Provider and third party documents or documents available on the Internet.

5.4 Procedures for obtaining audit records

The provider must record and keep available for the necessary period, including after the activity has ceased, all relevant information relating to the QCs issued.

The provider must record the exact time in the trust service delivery system. The time recorded for each event must be synchronized with UTC at least every 24 hours.

5.4.1 Types of recorded events

The following significant events must be recorded and evaluated by the provider:

- processes related to the Provider's key lifecycle (generation, backup, recovery, disposal, etc.),
- data obtained while providing trust services from Customers/Recipients,
- processes related to the HSM module itself,
- system logs of individual parts of the Provider's system

5.4.2 Frequency of processing of audit records

Provider administrators are required to continuously monitor submitted system logs to detect potential threats to the provider's service delivery in a timely manner. All recorded logs in electronic form must be stored on recordable media at regular intervals, at least once a month, so that they can be made available to auditors. Similarly, all written records of processes related to the lifecycle of the Provider's CA keys, timestamp authorities and OCSP Responder keys must be available to auditors.

5.4.3 Retention period of the audit report

The provider must keep audit logs in accordance with the requirements of the legislation currently in force. The audit logs must also be kept at least until the time of the next periodic external audit of its services.

5.4.4 Audit log protection

Audit records must be protected and stored in such a way as to prevent their deterioration, preferably in multiple copies located in different areas.

5.4.5 Audit log backup procedures

No provisions.

5.4.6 Audit collection system (internal vs. external)

No provisions.

5.4.7 Notification of the entity initiating the audit

No provisions.

5.4.8 Vulnerability assessment

See point 5.4.2.

5.5 Archive of records

5.5.1 Types of archived records

The Provider must keep all records of the issued QCs as well as the QCs themselves for the period specified in clause 5.5.2 in accordance with the requirements of the current legislation in force.

Records may be kept in paper or electronic form as required by law. The stored records must also include all documents that the Customer must submit to be issued the required type of certificate (e.g. extract from the commercial register, power of attorney, confirmation of ownership of the domain, etc.).

The provider must also keep all audit records (logs), written records of CA events (generation of CA keys, certificates for OCSP responders, etc.).

5.5.2 Retention period for the archive

The Provider must keep the original application for the issue of a QC together with the relevant documents confirming the identity of the Holder in paper or electronic form for at least 10 years.

5.5.3 Archive protection

The Provider's archival records must be stored in a secure location away from the premises and maintained in a manner that prevents unauthorized modification, destruction, or replacement.

5.5.4 Archive backup procedures

No provisions.

5.5.5 Time stamp requirements for records

No provisions.

5.5.6 Archiving system

No provisions.

5.5.7 Procedures for obtaining and verifying archival information

No provisions.

5.6 Key change

The whole process must be carried out without negatively affecting the level of security.

A change of the Provider's keys may occur for the following reasons:

- The expiration time of the Provider's keys currently in use is approaching. This is the normal state - 14 days before the expiration of the Provider Key Pair currently in use, a notice of the upcoming change of Provider Keys must be published on the Provider's website. Once a new key pair has been generated and a new certificate for the Provider has been produced, this must be published on the Provider's website.
- It is necessary to replace the Provider's keys currently in use due to their compromise. This is an exceptional, emergency situation - the Provider must immediately notify the Supervisory Authority (within 24 hours at the latest), all Holders of issued QCs and the public that the Provider's keys have been compromised. It must also immediately revoke the compromised certificate as well as all valid QCs signed with the compromised key. The Provider must notify, via its website, the Holders of QCs that have been signed with a revoked Provider Certificate as well as the Relying Parties that the revoked Provider Certificate is to be removed from each application used by the Relying Parties and replaced with a new Provider Certificate.

5.7 Recovering from compromise and disaster

5.7.1 Procedures for dealing with compromise and disasters

To ensure the integrity of the services, the Provider must implement data backup and recovery procedures.

The provider shall have recovery plans and emergency procedures in place for the provision of trust services.

Trusted services should be provided from two geographically separated CA systems, one of which is maintained as the main system and the other as a backup in case of a crash or failure of the main one.

Disaster and recovery procedures must be regularly tested and reviewed (at least on an annual basis) and should be updated and revised as necessary.

5.7.2 Computing resources, software or data are corrupted

In the event of damage or suspected damage to hardware, software or data, the Provider must use procedures designed to restore the damaged assets. The procedures must include activities to ensure a complete recovery of the environment.

5.7.3 Private key compromise procedures

In the event of compromise of the CA private key, the Provider must have procedures in place to restore a secure environment, procedures for distributing the public key to end users, and how new certificates will be issued to individual end users.

5.7.4 Maintaining business continuity after a disaster

The provider must have procedures in place to ensure business continuity in the event of an emergency caused by, for example, a natural disaster, to ensure its ability to resume operations. Procedures must include the location of the recovery site, procedures to protect assets at the disaster site, etc.

5.8 Termination of CA or RA

In the event of termination of the Provider's activities for reasons other than events of force majeure (e.g. natural disaster, state of war, decision of a public authority, etc.), the procedure shall be in accordance with point 5.7.

Before terminating the provision of services, the provider must:

- give appropriate notice, at least 6 months in advance, of the planned cessation of its activities to the Supervisory Authority, the Holders of any valid QCs issued by it, the parties relying on the QCs and the public,
- terminate any mandate agreements, powers of attorney, etc. under which other persons may have acted on behalf of the Provider (e.g. to provide RA services),
- revoke all valid QCs prior to termination if it fails to ensure the continuity of provision its services,
- attempt to enter a contract with another qualified trust service provider to ensure the continuity of provision its qualified trust services,
- concentrate and archive all the Provider's documents,
- to check compliance with the personal data protection regulations, i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data and on the free movement of such data and Act No. 18/2018 Coll. on the protection of personal data,
- disable all private keys, including copies thereof, in such a way that they cannot be recovered in any way.

If the reason for the termination of the Provider's activity is some reason unrelated to security, then neither the certificates of the issuing CAs that are terminating, nor the QCs signed by those CAs need to be revoked.

Upon termination of its activity, the Provider must ensure that the CA's signature data (private keys) cannot be demonstrably reused and must not issue any QCs.

The provider must have a solution to cover all costs associated with meeting the minimum termination requirements in the event of bankruptcy or other reason where the provider is unable to cover the costs from its own resources, in accordance with applicable bankruptcy law.

6 Technical security measures

The technical part of the Provider's infrastructure (hardware and software) must consist only of legal software and secure systems. The Provider's infrastructure architecture must be designed using components that meet state-of-the-art security standards.

Particular attention must be paid to the cryptographic module (HSM module) used to store, generate, and use the Provider's private keys. The cryptographic module (HSM module) is one of the most sensitive assets. The Provider's private keys must be stored in an HSM module that is certified to at least FIPS 140-2 Level 3.

The provider must use a combination of logical, physical, and procedural measures to protect its private key to ensure its security. These measures must be described e.g. in the issued CPS.

The Provider's system must include facilities for the continuous monitoring, detection and signaling of unusual and unauthorized attempts to access its resources.

Applications related to certificate status information shall be secured to prevent any unauthorized attempts to modify certificate status information.

All functions of the Provider that use a computer network must be secured against unauthorized access and other malicious activities.

6.1 Generating and installing a key pair

6.1.1 Generating key pairs

The generation and installation of the Provider's key pair must be performed in a standardized manner, which is described in detail in the Provider's documentation. The method of generation shall provide sufficient confidence in the generation process. The entire process of the generation method shall be recorded in writing. The generation of keys must be carried out by Provider staff in roles authorized to participate in the generation ceremony. Key generation must be performed in a secure cryptographic key storage facility that meets the legislative requirements for this type of facility.

6.1.2 Delivery of the private key to the subscriber

Not applicable

6.1.3 Delivery of the public key to the certificate issuer

Not applicable

6.1.4 Delivery of the CA public key to relying parties

Not applicable

6.1.5 Key sizes

A recommended key pair length or minimum key length must be specified for all entity types and all algorithms used (e.g. RSA).

6.1.6 Public parameter generation and quality control

The quality and parameters of the Provider's public keys must be determined by the PMA. The established parameters must be respected during the key generation ceremony. The Provider shall use FIPS 140-2 Level 3 compliant cryptographic hardware modules for key generation and storage that ensure random generation of RSA keys of at least 4096 bits.

For each type of QC made for end users, the Provider must have specified the quality and parameters of the public key (length, type) and must check their compliance before the actual release.

6.1.7 Key Uses (by X.509 v3 key use field)

The Provider's CA certificates must contain extensions that specify what the certificates can be used for.

6.2 Private key protection and cryptographic module design

6.2.1 Cryptographic module standards and controls

The Provider must use hardware cryptographic modules that are certified to FIPS 140-2 Level 3 to protect the private keys of its issuing CAs. The modules shall be stored in secure areas to which only persons in trusted roles have access.

The Provider's private keys may be used exclusively for signing certificates and CRLs issued by the Provider.

CA equipment must be always protected from unauthorized access, including unauthorized physical access.

6.2.2 Private key (n of m), multi-person control

For Provider private key management operations (e.g. backup, generation, destruction), the appropriate number of authorized persons must be always present on a "K" of "N" designated authorized persons basis (4 of 8).

6.2.3 Saving the private key

No provisions.

6.2.4 Private key backup

The Provider's private keys are generated and stored inside hardware cryptographic modules. If they need to be transmitted for the backup and recovery process, the private keys must always be transmitted in encrypted form. The transfer of private keys and their recovery in another hardware cryptographic module may only be carried out by authorized personnel in accordance with the rules set out in point 6.2.2.

6.2.5 Private key archive

No provisions.

6.2.6 Private key transfer to or from the cryptographic module

See 6.2.4

6.2.7 Storing the private key on the cryptographic module

Provider private keys, which are used in the creation of issued qualified certificates for end-users, can be stored in the HSM itself in a readable form. All provider HSMs shall be operated in secure premises with regime access.

6.2.8 How to activate the private key

The Provider's private keys may only be activated by authorized persons within the meaning of clause 6.2.2.

During activation, each authorized person from the required number of authorized persons must insert his/her smart card into the HSM module and enter the password for it.

After activation, the keys in the HSM module are active until they are deactivated by an authorized person (CA administrator) or until the HSM module's power supply fails.

Holders of private keys to whom the Provider has issued a QC for the respective public key are solely responsible for the protection of their Holders' private keys.

6.2.9 How to deactivate the private key

Deactivation of the private key in the HSM module can only be performed by an authorized person (CA administrator) or by power failure of the HSM module or the keys are deactivated automatically when the sessions fail.

6.2.10 Method of destroying the private key

The provider shall ensure by technical and organizational measures that the private keys of the provider's issuing CAs cannot be used after the end of its life cycle. A record shall be made of the end of the CA private key lifecycle and the technical and organizational measures taken, signed by all actors present.

6.2.11 Cryptographic module evaluation

See point 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public Key Archive

The Provider must keep all public keys for which it has been issued a certificate in accordance with clause 5.5.2

6.3.2 Certificate operating periods and key pair usage periods

The validity of the QCs produced by the Provider and the usability of the key pair must not exceed the following values:

Type of certificate	**Validity (maximum)**
Issuing CA	30 years
QC for the end user	1 year

6.4 Activation data

6.4.1 Generating and installing activation data

The QC holder's activation information (password and OCRA token or activated NFQES Qualified Authenticator application - software OCRA token) associated with the specific QC holder must be submitted during the face-to-face meeting when the QC is issued. The holder shall be informed of the manner and need to change them and of the risks if those changes are not made. The activation data may take the form of an S/N token, a PIN or a password divided into several parts based on the k/n principle, etc.

The activation data for the cryptographic modules used by the Provider's CA must be created in accordance with clause 6.2.2.

6.4.2 Activation of data protection

Holders are solely responsible for the protection of their private access data and PINs to the Holders' hardware token.

When the QC for the website is made, Holders must be advised by the Provider of the need to protect the private key with a strong password to authenticate the website, so that it cannot be misused during the entire period of its use.

Key pair intended for the QC publisher:

- must be generated in a security module that meets the minimum requirements of FIPS 140-2 level 2,
- any manipulation of the private key may only be allowed under the principle of multiple control, the minimum number of authorized persons required being four (4).

6.4.3 Other aspects of activation data

It must be ensured that the private keys of the issuing CAs never get in unencrypted form outside the module where they are stored.

No one is to have access to the private signature key except the Holder.

PINs, pass-phrases, biometrics, or other mechanisms of equivalent authentication robustness must be used to protect access to the use of the private key.

Activation data for private keys belonging to certificates confirming individual identity must never be shared.

The activation data for private keys belonging to certificates confirming the identity of an organization shall be known only to those authorized in the organization to use the private keys.

6.5 Computer security checks

6.5.1 Specific technical requirements for computer security

The Provider must perform all functions of a qualified trust service provider using a trusted system that meets the requirements defined in the Provider's IS security design.

A provider issuing QCs may be guided in the provision of its services by the information security requirements for a trust service provider as defined in 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.

All systems must be regularly checked for malicious code and protected against spyware and viruses.

6.5.2 Computer security assessment

No provisions.

6.6 Life cycle measures

6.6.1 System development checks

The Provider's applications for the Provider's system needs shall consider the measure of security of the development environment, personnel security, configuration management security in the maintenance of systems, within the technical software development procedures, within the software development methodology and layering and its modularity.

6.6.2 Safety management controls

The Provider must use tools and procedures to determine whether the operating systems used within the Provider's CA and the network connections used still meet the set level of security.

These tools and procedures should include checking the integrity of security software, firmware, and hardware to ensure they are working properly.

6.6.3 Life cycle safety measures

No provisions.

6.7 Network security controls

The Provider must have measures in place to ensure network security, including the security of firewalls.

6.8 Time stamp

The Provider shall purchase time stamps from external entities that have the status of a qualified trust service provider and provide a qualified trust service for the execution of a qualified electronic time stamp within the meaning of the provisions of Regulation (EU) No 910/2014 (eIDAS). These time stamps will be used in the Application, in the SIGNING section, when signing QC documents. If the Customer/Recipient is interested, he/she can also order a qualified trust service for storing qualified electronic signatures/seals, where, after signing a document, this signature/seal is stored with the Provider together with the calculated hash of the document with an internal time stamp (ISO 14533-4 - TStOCSP), while at regular intervals, still during the validity of the previous time stamp, in order to prolong the trustworthiness of the qualified electronic signature and the seal also for the period after the expiration of their technological validity.

6.9 Qualified electronic signature/seal storage service

The process for storing signatures and seals will meet the requirements according to ETSI document TS 119 511 V1.1.1 (2019-06) using the Temporary Storage Service with internal time stamp (according to ISO 14533-4 - TStOCSP).

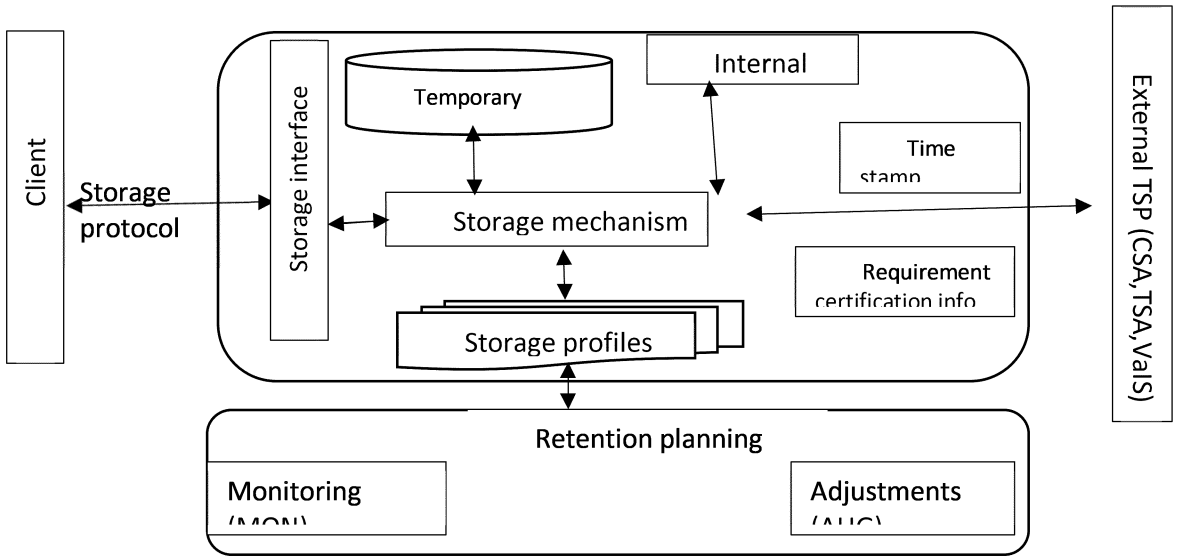
The Qualified Electronic Signature/Seal Temporary Storage Service will store one or more calculated hash values from files received from the Customer. The service may, at the Customer's initiative, also store all files received from the Customer in addition to the calculated hash values.

The retention service will make available to the Customer the evidence and files received, if the Customer has requested such service, for the period requested by the Customer and agreed to by the Provider. Once the preservation service has produced the evidence, the Customer will have access to that evidence upon request through the application for the time of the preservation of the evidence. This period may be extended by mutual agreement between the Customer and the Provider.

The storage service may contact external trust service providers to obtain the information needed to create the evidence to be stored. These may be external Certificate Authorities (CAs), external Time Stamp Authorities (TSAs), external Signature or Seal Creation Services (SigS) or Validation Services (VaIS).

The preservation service will use an internal or external timestamp authority for the creation of preservation evidence.

The storage service will monitor the cryptographic algorithms used inside its active profiles and change the group of algorithms used if necessary (for example, if a vulnerability is found). The stored evidence will be created according to the active profiles and modified if necessary.


Client
Storage protocol
Storage interface
Temporary
Internal
Time stamp
Storage mechanism
Requirement certification info
Storage profiles
External TSP (CSA,TSA,ValS)
Retention planning
Monitoring (MON)
Adjustments (AUC)

7 Certificate, CRL and Processes OCSP

7.1 Certificate Profile

QC profiles, Certificate Revocation List (CRL) profiles and the response in the form of certificate validity information provided via the OCSP protocol shall be centrally determined by the PMA and neither the service level (role) holders can arbitrarily change the structure of these profiles or responses.

According to Article 28(3) and Article 38(3) of the eIDAS Regulation, qualified certificates for electronic signatures (seals) may contain optional additional specific attributes. These attributes do not affect the interoperability and recognition of qualified electronic signatures (seals). Similarly, a certificate for web site authentication may contain optional additional specific attributes as long as these attributes do not affect the interoperability and recognition of these qualified certificates.

The structure of the QC produced by the provider may only be changed at the discretion of the PMA's delegated member.

7.1.1 Version numbers

This CP only allows QC profiles compliant with the X.509 version 3 standard.

7.1.2 Certificate parameters

Version (Version)	V3 (value 0x2)
Serial number	Unique number assigned by the Provider > 0
Issuer Signature Algorithm	sha256WithRSAEncryption (1 2 840 113549 1 1 11)
Issuer	Unique X.500 distinguished name of the Provider
Valid from (Valid from)	Start of certificate validity (UTC time)
Valid to (Valid until)	Certificate expiration (UTC time)
Subject ()	See section 7.1.5.1; 7.1.5.2; 7.1.5.3; 7.1.5.4 for the content of the individual items for each type of QC
Public key	The public key for which the certificate is made (min size 3072 bit)
Extensions	See Table 5 for a list of extensions in QC

7.1.3 Certificate Extension

Name of the extension	ASN.1 Name and OID/Description	Presence	Criticality
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Specifies (http:// ... p7c, certificate or also ldap://...) the address to obtain certificates issued for the issuer of this certificate and the address to OCSP.	Yes	No
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14}	Yes	No

	The Certificate Holder's public key identifier.		
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} The public key identifier of the CA that issued this certificate.	Yes	No
certificatePolicies	{id-ce-certificatePolicies} {2.5.29.32} Identifies the certification policies under which the certificate was issued.	Yes	No
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Specifies how and from where a CRL can be obtained.	Yes	No
QCstatements	{id-pe-qcStatements} {1.3.6.1.5.5.7.1.3} A specific statement regarding the EU Qualified Certificate: esi4-qcStatement-1 esi4-qcStatement-2 esi4-qcStatement-4 esi4-qcStatement-5 esi4-qcStatement-6	Yes	No
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifies the type of certificate (end entity, CA).	Yes	Yes
keyUsage	{id-ce-keyUsage} {2.5.29.15} Defines the purpose for which the private key whose public key is part of this certificate is used.	Yes	Yes
extKeyUsage	{id-ce-extkeyUsage} 2.5.29.37 Defines the extended use of the private key whose public key is part of this certificate.	Yes in QC for website authentication	No
SubjectAltNames	{id-ce-subjectAltName} {2.5.29.17} This extension contains one or more alternate names, using any of a range of name forms for the entity that is bound by the CA to the public key.	Yes in QC for website authentication	No

7.1.4 Algorithm object identifiers

Signature Algorithm for QCs (Signature Algorithm)

sha256RSA OID: 1.2.840.113549.1.1.11

7.1.5 Forms of names

For a natural person, the first name/s in the givenName (GN) field and the last name/s in the Surname (SN) field must be entered in the QC for the electronic signature. First Name/s and Surname/s together in the form specified by the Holder/Customer shall still be entered in the commonName (CN) field.

For a legal entity, the QC for the electronic seal must contain its official name in the Organization field and its other identifier, if any, in the organizationIdentifier or serialNumber or both.

For a Web site, the QC for authenticating the Web site must specify the exact domain name (FQDN) in the CN field and in the subjectAltName extension.

The certificate of the issuing CA must always include the Provider identifier in the form "CA NFQES".

The structure of the certificates issued by the Provider may only be changed at the PMA's discretion.

Key lengths and QC validity: public key

- RSA, minimum length 3092 bits
- EC, minimum length 256 bits

7.1.6 Restrictions on names

No provisions.

7.1.7 Certification policy identifier

See chapter 1.2

7.1.8 Using extensions to restrict the policy

This extension is not used.

7.1.9 Syntax and semantics of politics

Each QC issued in accordance with this policy shall contain its identifier in the form of an OID (see clause 1.2) in the id-ce-certificatePolicies extension (2.5.29.32).

In addition, each SSL certificate must contain an identifier in the form of an OID (2.23.140.1.2.2.2) that the certificate is made as an SSL certificate where the organization (legal entity or natural person) that has control of the exact domain name (FQDN) specified in it has been authenticated.

7.1.10 Extension

No provisions.

7.2 Profile of CRL

7.2.1 Version numbers

CRLs issued by the Provider must be CRL version 2.

CRLs must be issued by the same CA of the Provider as the certificate.

The CRLs issued must comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

7.2.2 CRL and CRL input extensions

Extensions to the CRL issued

Name of the extension	Required	Criticality
Authority Key Identifier (OID: 2.5.29.35)	YES	NO
CRL Number (OID: 2.5.29.20)	YES	NO
Issuing Distribution Point (OID: 2.5.29.28)	YES	YES
id-ce-expiredCertsOnCRL (OID: 2.5.29.60)	YES	NO

7.3 Profile of OCSP

7.3.1 Version numbers

If the Provider issues OCSP responses, these must be in accordance with RFC 6960 "X.509 Internet Public Key Infrastructure (PKI) Online Certificate Status Protocol - OCSP". If OCSP responses will be issued by separate OCSP responders for each of the Provider's CAs issuing QCs, their signing certificates shall be signed by the corresponding Provider CAs and shall include an extension for the use of the OCSP Signing Key (1.3.6.1.5.5.5.7.3.9).

7.3.2 OCSP Extensions

Extensions in the OCSP response

Name of the extension	Required	Criticality
id-commonpki-at-certHash (OID: 1.3.36.8.3.13)	YES	NO
id-pkix-ocsp-nonce (OID: 1.3.6.1.5.5.7.48.1.2)	NO	NO
id_pkix_ocsp_archive_cutoff (OID: 1.3.6.1.5.5.7.48. 1.6)	YES	NO

8 Audit compliance and other assessments

The purpose of the audit is to confirm that the Provider as a qualified trust service provider and the qualified trust services it provides meet the requirements set out in the eIDAS Regulation.

8.1 Frequency or circumstances of assessment

The provider shall be audited at least every 24 months on the qualified trust services it provides.

8.2 Identity/qualifications of the assessor

The conformity assessment body and its authorized auditors shall comply with the requirements of ETSI EN 319 403 "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers" at least in version 2.2.2 in accordance with the NBÚ certification scheme that governs the requirements of this standard.

8.3 Relationship of the evaluator to the evaluated entity

The person auditing the Provider shall comply with the Auditor Code of Conduct as defined in Annex A of ETSI EN 319 403 at least in version 2.2.2.

8.4 Topics covered by the evaluation

The purpose of the audit is to confirm that the Provider as a qualified trust service provider and the qualified trust services it provides meet the requirements set out in the eIDAS Regulation.

8.5 Measures taken as a result of the shortfall

When the auditor identifies a discrepancy between the Provider's operations and the applicable requirements or provisions of the CP and issued CPS, the following actions must be taken:

- the auditor must notify the entities defined in paragraph 8.6 of the discrepancy,
- the discrepancy must be recorded,
- The PMA must determine the appropriate remedial action.

8.6 Announcement of results

The conformity assessment body must submit the results of the audit in writing to the audited body, which must implement and take the necessary corrective actions based on the results. The implementation of the corrective measures shall be brought to the attention of the conformity assessment body.

Within three (3) working days of its receipt, the Provider is obliged to submit the resulting conformity assessment report to the Supervisory Authority.

9 Other business and legal matters

9.1 Fees

It is the Provider's obligation to publish in an appropriate manner the valid price list of its qualified trust services or information on which contractual conditions it is possible to obtain qualified trust services.

Fees for qualified trust services provided by the Provider shall be paid by the Customer.

9.1.1 Fees for the issue or renewal of a certificate

The Provider publishes the current price list of its services via its website (see Chapter 1).

The Provider may also agree the prices of certificates with the Customer individually, e.g. based on a contract or a quotation and a binding order. In such case, the general price list shall not apply to the provision of the Provider's services.

If the Provider's QC are issued through an external registration authority, this registration authority is obliged to charge the price for the QC according to the Provider's valid price list. The RA may charge additional fees on its behalf, e.g. related to the mediation of the service.

9.1.2 Fees for access to the certificate

The Provider shall provide online access to information on issued QC free of charge to the Cooperating Parties via its website (see Chapter 1).

9.1.3 Fees for appeal or access to status information

The Provider provides a free certificate revocation service as well as a certificate status verification service consisting of issuing CRLs and OCSP responses to the Cooperating Parties.

9.1.4 Charges for other services

The Provider may also charge fees for other associated trust services requested by the Customer in accordance with the applicable price list or based on an individual agreement with the Customer.

9.1.5 Refund Policy

The Provider may refund payment for services provided to the Customer in justified cases, based on a reasoned request by the Customer and its individual assessment.

9.2 Financial responsibility

The provider must have sufficient resources to perform the trust services it provides and/or obtain appropriate liability insurance to remain solvent and, if necessary, be able to indemnify in the event of a court decision or settlement in relation to the provision of those services.

9.2.1 Insurance cover

The Provider must be insured against possible damages that may be caused to Certificate Holders or third parties in connection with the provision of trust services.

9.2.2 Other assets

No provisions.

9.2.3 Insurance or guarantee for end-users

No provisions.

9.3 Confidentiality of business information

Both the Customer and the Provider are obliged to access the data obtained in connection with the provided qualified trust services in accordance with the relevant legislation.

9.3.1 Scope of confidential information

Confidential information subject to appropriate protection is:

- internal infrastructure (e.g. documents, procedures, files, scripts, passwords, pass-phrases, etc.) used for the operation of the Provider, including its RA, the Provider's private keys used for signing the executed QCs,
- OCSP responder private keys used to sign responses to requests to confirm the existence and validity of the QC,
- personal data of Certificate Holders subject to protection under the Personal Data Protection Regulations.

and, where applicable, other technical, commercial, or manufacturing data or other information which is not publicly available, and which is marked as confidential by the Customer or the Provider. Confidential information may include, but is not limited to, data, specifications, analyses, commercial information, know-how, documentation, procedures and processes, information relating to clients or business partners or other information from the Provider's or its Customers' information system in any form.

All confidential information is to be treated as sensitive information and access to it is to be restricted to those who strictly need the information to carry out their duties.

9.3.2 Information which does not fall within the scope of confidential information

Confidential information is not, or ceases to be, information that:

- are publicly available at the time of their receipt by the other Party or become so later without the other Party having breached its obligations under this Policy; or
- were known to the other party by their disclosure in connection with the trust services provided, or
- has been demonstrably obtained by the other party from a third party who is demonstrably authorized to disseminate such information; or
- have been independently developed by the other party without tampering with confidential information; or
- are common knowledge despite their designation as confidential by the other party.

9.3.3 Responsibility for the protection of confidential information

Both the Provider and the Customer are obliged to protect confidential information from disclosure and to refrain from using it or disclosing it to a third party in the event of obtaining confidential information or accessing it.

If confidential information is to be disclosed or made available to a third party in the performance of its activities for the Provider, the Provider shall be required to enter into a confidentiality or non-disclosure agreement with the third party, which shall include the obligations set out above.

The Provider may disclose certain confidential information to a third party in certain circumstances, in the case of:

- compulsory disclosure in criminal, civil or administrative proceedings,
- mandatory provision of information to the supervisory authority,

- the provision of information at the request of the data subject.

9.4 Privacy Policy

9.4.1 Data Protection Plan

The Provider must comply with the requirements of the Personal Data Protection Regulations when processing personal data.

The Provider shall ensure the confidentiality and integrity of the personal data obtained in the process of issuing a QC, including in the case of their transfer between the Customer and the Provider or between the individual components of the Provider's system.

The Provider will retain certain personal data to comply with its legal obligations and to ensure the operation of its business activities.

To informing the Holder/Customer about the processing of personal data carried out by the Provider in the provision of trust services, the Personal Data Processing Information is:

a) always available in electronic form on the Provider's website;

b) sent in electronic form to the Customer's/Holder's email address prior to the commencement of the provision of trust services; and

c) available in paper or electronic form from the Provider and individual RAs.

9.4.2 Information considered private

The Provider shall consider as private any personal data relating to an identified or identifiable natural person, such person being one who can be identified, indirectly or directly, by reference to a generally applicable identifier or to one or more characteristics or attributes which constitute his or her physical, mental, economic, physiological, physiological, mental, cultural, or social identity.

9.4.3 Information that is not considered private

The Provider may, in accordance with the Data Protection Regulations, define the types of information it processes in the provision of qualified trust services that are not considered personal data.

The Provider may make available or publish information about the issuance of a qualified certificate with the name of its Holder on its website based on the written consent of the Certificate Holder.

9.4.4 Responsibility for the protection of private information

The Provider shall securely protect and store the personal data processed in connection with the production of the QC. It shall protect such data by adopting appropriate security measures, against unauthorized access, disclosure, or alteration.

9.4.5 Notification and consent to the use of private information

The Provider is obliged to comply with the Personal Data Protection Regulations when fulfilling the information obligation towards the data subjects and when obtaining their consent to the processing of personal data.

9.5 Intellectual property rights.

The Provider is the copyright holder of all documents, procedures, procedures, rules, databases, policies, certificates, and private keys that are part of the Provider's infrastructure and that have been created by the Provider.

9.6 Declarations and warranties

The Provider, through this CP and the Certificate Issuance Agreement, expresses the legal prerequisites for the use of the issued QC by their holders and relying parties.

9.6.1 CA representations and warranties

No warranties or representations are made by the Provider with respect to the trust services provided, except as set out in this CP and the CPS that follow.

The Provider reserves the right to change these declarations as it deems appropriate, at its sole discretion or in accordance with applicable law.

To the extent set out in the individual parts of this CP or the CPS issued, the Provider declares:

- comply with its obligations under this CP, the issued CPS as well as other published policies and procedures, including the Information Security Policy,
- fulfilment of its obligations under the eIDAS Regulation and the applicable legislation of the Slovak Republic,
- immediately informing the subjects concerned in the event of compromise of their private keys in accordance with this CP,
- implementing security mechanisms, including mechanisms for private key generation and protection, relating to the protection of its PKI infrastructure,
- the availability of printed or electronic versions of this CP and other published policies online,
- the fact that the Holder becomes or is the owner of the private key at the time of execution of the Qualified Certificate under this CP,
- the accuracy of the information contained in the executed qualified certificates to the best of the Provider's knowledge and compliance of the issued qualified certificates with the requirements of the eIDAS Regulation,
- Compliance with the Data Protection Regulations in the handling of Holders' personal data.

9.6.2 RA Declaration and Warranties

The internal RA providing qualified trust services of the Provider declares the same representations and warranties as the CA (see chapter 9.6.1)

9.6.3 Declarations and warranties of participants

Except as otherwise provided in this CP or the relevant agreement with the Holder/Customer, the Holder shall be solely responsible for:

- generation of the key pair public/private key in case the key for the QC request is generated by the user,
- providing accurate and correct information in communication with the Provider,
- read and agree to all the terms and conditions set out in this CP and its associated policies, which are available on the Provider's repository (see Chapter 1),
- use of issued QCs only for legal and authorization purposes in accordance with this CP,
- terminate the use of the QCs if any information in them proves to be misleading, outdated, or incorrect,
- use its best efforts to prevent compromise, loss, declassification, modification, or any unauthorized use of the private key corresponding to the public key contained in the QC issued by the Provider.

9.6.4 Representations and warranties of the relying parties

See chapter 10 of the document GTC of provision and use of the trusted service of issuing and verifying certificates brainit.sk, s.r.o., the current version of which is available on the Provider's website (https://zone.nfqes.sk/).

9.6.5 Representations and warranties of other participants

No provisions.

9.7 Disclaimer of warranties

Pursuant to Article 13 of the eIDAS Regulation, the Provider shall be solely liable for damage caused by its failure to comply with its obligations under the eIDAS Regulation.

9.8 Limitations of liability

The Provider shall not be liable for consequential losses or indirect damages incurred by Customers or relying parties in connection with the use of the Trust Services.

The Provider shall not be liable for damages (including lost profits) incurred by the Certificate Holder/Customer, the Relying Party or any third parties due to:

a) breaches of obligations by the Certificate Holder/Customer or Relying Party set out in generally applicable law, the relevant contract, the GTC or the Provider's policies, including the obligation to exercise reasonable care in the use of and reliance on the Certificates,

b) failure of the Certificate Holder/Customer to provide the necessary cooperation,

c) the technical characteristics, incompatibility, configuration, unsuitability or other defects of the software or hardware used by them,

d) using or relying on a certificate that has expired or been revoked,

e) use of the certificate by the Certificate Holder/Customer in violation of the Contract, the GTC or the Provider's policies,

f) that the certificate has been used in violation of its designation, purpose or limitations specified in the certificate, in these GTC or in the Provider's policies,

g) non-delivery or delay of requests to verify the status of the certificate to the Provider, for reasons that are not on the Provider's side (in particular, cases of unavailability or congestion of the Internet network or defects in the equipment or technical equipment used by the verifier),

h) failure to provide any of the trusted services or their unavailability during planned maintenance or reorganization announced on the Provider's website,

i) the action of a higher power,

The Provider shall not be liable for damages incurred by the Relying Party because of non-compliance with Chapter 10 of the GTC and these CP when relying on the Provider's qualified certification and trust services or on a qualified electronic signature or seal made on the basis thereof, or on the Relying Party's Information.

From the moment when the device on which the private key to which the QC belongs is stored is acquired by the Holder, the Provider shall not be liable:

a) for the protection of the device on which the QC and the private key are stored, or for the protection of the access codes necessary for its use,

b) for the unauthorized person taking possession of the device or the private key,

c) for damages caused using the private key or the QC if the Holder/Customer does not act in accordance with his/her obligations, if the private key is seized by an unauthorized person and the Holder/Customer does not request the Provider to cancel the QC or if he/she does not notify the Provider of changes in the data.

9.9 Compensation

Whoever breaches his/her duty or any obligation arising from this CP, the Contract and the GTC is obliged to compensate for the damage caused to the other party, except in cases where the liability of the entity for damages is excluded. Damages shall be deemed to be actual damage, loss of profit and costs incurred by the injured party in connection with the damage event.

Whoever breaches his duty or any obligation arising from this CP, the Contract and the GTC, may be released from liability for damages only if he proves that the breach of duty or any obligation was due to circumstances excluding liability - force majeure.

9.10 Duration and termination

9.10.1 Deadline

This version of the CP is valid from the date of its entry into force, i.e. 1.12.2020, until it is replaced by a new version. Details of the change history of this CP are set out at the beginning of the document in the "Change History" section.

9.10.2 End

The validity of this version of the CP shall expire on the date of publication of a new version with a higher number than 3.0, or termination of the activity of provision of qualified trust services by the Provider at the time of its validity. All revisions to the CP and CPS that are listed in the change history for the document must be made available to Holders/Customers and/or Relying Parties.

9.10.3 Termination and survival effect

If this document is not replaced by a new version and at the time of its validity the provision of qualified trust services by the Provider is terminated, all provisions of this CP relating to the Provider shall be complied with and the Provider shall be obliged to comply with the provisions of this CP after the termination of its activity.

9.11 Individual notifications and communication with participants

The Provider's communication with the internal RA must be done officially via authorized email communication between the Provider's designee and the RA's designee.

9.12 Amendments

9.12.1 Amendment procedure

Updates to the CP shall be made based on its review, which shall be carried out at least once a year from the approval of the version currently in force. The review must be carried out by an authorized employee of the Provider who must, based on the results of the review, draw up a written proposal for any proposed changes.

Approval of the proposed changes must be made by an authorized PMA member. Proposed changes must be considered within 14 days of receipt. After the expiration of the time limit for

consideration of the proposed change, the PMA must accept, accept with modification, or reject the proposed change.

Errors, update requests or proposed changes to the CP shall be communicated to the contact referred to in clause 1.5.2. Such communication shall include a description of the change, the rationale for the change and the contact details of the person requesting or proposing the change.

All approved changes to the CP must be brought to the attention of the entities concerned within one week prior to their entry into force, through the publication and notification policy channels (see paragraph 2.2).

Each changed version of this CP must be numbered and filed so that the newer version has a higher version number than the one it replaces.

Corrections of typos, grammatical and stylistic errors shall not be considered as changes initiating a version change of this CP.

9.12.2 Mechanism and notification period

The provider must publish information regarding the current version of the CP via its website (see Chapter 1).

The Provider's authorized representative must inform all the Provider's contracted RAs of the approval of the new version of the CP by sending an email version of the CP prior to its entry into force in accordance with clause 9.12.1. The Provider must request feedback from the RAs in the form of a confirmation email of receipt of the electronic version of the Provider's CP.

The current version of the CP must be available on each contracted RA of the Provider at least in electronic form. Internal staff must be equally informed of the new version of this CP.

9.12.3 Circumstances in which the OID must be changed

Each policy must have its OID set by the Provider. The OID of this policy is specified in clause 1.2 and remains unchanged for each new minor version of the CP.

9.13 Dispute resolution provisions

The Holder/Customer has the right to send the Provider a complaint, suggestion or claim about the qualified trust service provided by email to ca@nfqes.sk. The Provider shall handle the complaint no later than within 30 days of its receipt unless the parties agree otherwise. The handling of the complaint relates only to the description of the defect given by the Customer.

The courts of the Slovak Republic shall have exclusive jurisdiction to adjudicate any disputes between the Provider and the Certificate Holder/Customer. If the Certificate Holder/Customer is a consumer, any dispute may also be settled out of court.

In this case, the customer is entitled to contact the out-of-court dispute resolution entity, which is the Slovak Trade Inspection, or another legal entity registered in the list of alternative dispute resolution entities maintained by the Ministry of Economy of the Slovak Republic and available on its website. The Holder/Customer has the right to choose which of the above mentioned alternative dispute resolution entities to turn to. Before proceeding to judicial or out-of-court dispute resolution, the Parties are obliged to first try to resolve the dispute by mutual agreement.

9.14 Applicable law

Legal relations between the Provider and the Certificate Holder/Customer are governed by the laws of the Slovak Republic.

The rights and obligations of the contracting parties not expressly provided for in the contract concluded between the Provider and the Customer, the GTC and this CP shall be governed by the relevant provisions of Act No. 513/1991 Coll., the Commercial Code, as amended, Act No. 40/1964 Coll., the Civil Code, as amended, and other generally binding legal regulations of the Slovak Republic.

9.15 Compliance with applicable legislation

The Provider provides trust services in accordance with the applicable legislation in force in the Slovak Republic.

9.16 Miscellaneous provisions

No provisions.

10 Links

- Regulation (EU) No 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/ES, Regulation (EU) No 910/2014 and Corrigendum
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data and on the free movement of such data
- Act No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amending and supplementing certain acts (hereinafter referred to as the Trust Services Act)
- Act No. 18/2018 Coll. on Personal Data Protection
- Information on the processing of personal data (version 1.0)
- General Terms and Conditions of Provision and Use of the Trusted Service for the Execution and Verification of Certificates brainit.sk, s.r.o. effective from 1.12.2020 (version 1.1)
- SD Supervisory scheme for qualified trust services as defined by the supervisor
- 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
- 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
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC6960)
- OCRA: OATH Challenge-Response Algorithm (RFC6287)