



B R A I N : I T

Policy of certification activities for NFQES CA – External Registration authority

Version: 1.0

Date of effect: 1.4.2022

PO-09

Policy

Public

Created by:

Ing. Martin Berzák
Security manager

1.4.2024

Approved by:


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

1.4.2022

brainit.sk, s. r. o.

Veľký Diel 3323, 010 08 Žilina
IČO: 52577465

www.brainit.sk

 NFQES BRAIN:IT	Version:	1.0
	Page:	2 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

History of changes

Version	Date	Authors	Description	Reason for changes
1.0	1.4.2022	Ing. Martin Berzák Ing. Michal Šterbák	First approved version of the document	



 NFQES BRAIN:IT	Version:	1.0
	Page:	3 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

TABLE OF CONTENTS


Definitions and acronyms	6
<i>Definitions.....</i>	<i>6</i>
<i>Acronyms</i>	<i>6</i>
1 Introduction.....	8
1.1 Overview.....	8
1.2 Title and identification of the document.....	9
1.3 PKI participants.....	10
1.3.1 Certification Authority.....	10
1.3.2 Registration Authority.....	10
1.3.3 End users	11
1.3.4 Relying parties	12
1.3.5 Other parties	12
1.4 Use of the certificates.....	13
1.4.1 Appropriate use of certificates	13
1.4.2 Basic use of certificates	13
1.5 Contact information	13
1.6 Policy governance.....	14
1.6.1 Organization responsible for policy governance	14
1.6.2 Contact	14
1.6.3 Supervisory authority.....	14
2 General provisions	15
2.1 Obligations	15
2.1.1 Duties of the RA.....	15
2.1.2 Obligations of the certificate Holder.....	16
2.1.3 Obligations of the relying parties.....	17
2.2 Legal warranties.....	17
2.2.1 Provider declarations and warranties – NFQES CA.....	17
2.2.2 RA declarations and warranties	18
2.2.3 Declarations and warranties of participants	18
2.2.4 Declarations and warranties of the relying parties.....	18
2.2.5 Declarations and warranties of other participants	18
2.3 Financial responsibility	18
2.3.1 Insurance cover	18
2.3.2 Other assets.....	18
2.3.3 Insurance or guarantee for end-users	18
2.4 Arbitration and dispute resolution	19
2.4.1 Dispute resolution provisions	19
2.4.2 Governing law	19
2.5 Fees.....	19

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------


 NFQES BRAIN:IT	Version:	1.0
	Page:	4 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

2.6	<i>Disclosure and storage</i>	19
2.6.1	Disclosure of CA information	19
2.6.2	Frequency of publication of information	20
2.6.3	Access controls.....	20
2.6.4	Storage	20
2.7	<i>Compliance audit</i>	20
2.7.1	Frequency of compliance audit for a given entity	20
2.7.2	Auditor identity and qualification requirements	21
2.7.3	Topics covered by the compliance audit.....	21
2.7.4	Actions taken to correct deficiencies	21
2.7.5	Handling of audit results	22
2.8	<i>Secrecy</i>	22
2.8.1	Types of protected information	22
2.8.2	Circumstances of release of confidential information.....	22
2.9	<i>Intellectual property rights</i>	23
3	Identification and authentication	24
3.1	<i>Initial registration</i>	24
3.1.1	Types of names.....	24
3.1.2	The need for meaningful names	24
3.1.3	Uniqueness of names.....	24
3.1.4	Dispute resolution procedure for name clashes.....	24
3.1.5	Recognition, authentication and the role trademarks.....	24
3.1.6	Proving private key ownership.....	24
3.1.7	Authentication of the identity of the legal entity (organization)	25
3.1.8	Authentication of the identity of a natural person.....	26
3.1.9	Device, system or website identity authentication	27
3.1.10	Identity authentication with contractors	28
3.1.11	Documents to be presented	28
3.1.12	Verification of data on documents submitted	30
3.1.13	Initial registration of RA	31
3.2	<i>Issue of a subsequent certificate</i>	32
3.3	<i>Issuance of a subsequent certificate after revocation of the old one</i>	32
3.4	<i>Application for revocation of a certificate</i>	32
4	Operational requirements	33
4.1	<i>Applying for a certificate</i>	33
4.1.1	Who can apply for a certificate	33
4.1.2	Procedure for obtaining a certificate	33
4.2	<i>Issuance of the certificate</i>	34
4.2.1	Delivery of the private key to the certificate Holder	35
4.2.2	Delivery of the CA public key to users.....	35

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	5 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

4.3	<i>Receipt of the certificate</i>	35
4.4	<i>Certificate suspension and certificate revocation</i>	35
4.4.1	<i>Certificate revocation</i>	35
4.4.2	<i>Suspension of the certificate</i>	38
4.4.3	<i>Certificate revocation list</i>	38
4.4.4	<i>Verification of current certificate status</i>	38
4.4.5	<i>Other applicable means of notification of certificate revocation</i>	39
4.5	<i>Security audit</i>	39
4.5.1	<i>Types of events to be recorded</i>	39
4.6	<i>Archival records</i>	39
4.7	<i>Changing the key</i>	40
4.8	<i>Contingency plan for emergencies</i>	40
4.9	<i>Termination of CA or RA</i>	41
5	Physical, procedural and personnel security measures	43
5.1	<i>Physical security measures</i>	43
5.2	<i>Procedural security measures</i>	43
5.3	<i>Personnel security measures</i>	44
6	Technical security measures	45
6.1	<i>Key pair generation and installation</i>	45
6.1.1	<i>Key pair generation</i>	45
6.1.2	<i>Delivery of the private key to the certificate Holder</i>	45
6.1.3	<i>Key length</i>	45
6.2	<i>Private key protection</i>	46
6.3	<i>Key pair management</i>	46
7	Certificate profiles and list of revoked certificates	47
7.1	<i>Certificate profiles</i>	47
7.2	<i>Certificate Revocation list profiles</i>	47
8	Administration of specifications	48
8.1	<i>Specification change procedures</i>	48
8.2	<i>Publication and notification policy</i>	48
8.3	<i>Publication procedures</i>	48
8.4	<i>Concessions</i>	48

 NFQES BRAIN:IT	Version:	1.0
	Page:	6 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Definitions and acronyms

Definitions

For the purpose of this document, the following terms and definitions are used:

Contracting Partner – is a legal entity (PO) or natural person (FO) with whom brainit.sk, s. r. o. has concluded a written contract for the issuance and use of the NFQES CA certificate and services.

Registration authority or RA – is an entity that, in accordance with the NFQES CA Certification Policy (NFQES CA CP) and/or the policy of its subordinate Certification Authority (CA) NFQES ACA (NFQES ACA CP) in the current and valid version, As a Registration Authority (RA), on behalf of the NFQES CA, performs selected certification activities in the provision of NFQES CA or NFQES ACA trust services, as applicable, and brokers NFQES CA/NFQES ACA services to Certificate Holders and Certificate Applicants.

Certificate – for the purposes of this document means any Certificate that is issued for the Trust Service being provided by an NFQES CA/NFQES ACA (as defined in Regulation 910/2014 eIDAS). A certificate is issued by an RA on behalf of the NFQES CA/NFQES ACA to users of the electronic portal <https://www.zone.nfqes.com>

Certificate Holder – means the person named in the Certificate as the holder of the private key associated with the public key to which the Certificate is issued.


Applicant of the Certificate – s a person who applies for the issuance of the Certificate and based on identification documents the identity of the person is verified. The applicant and the certificate holder are usually the same person.

Acronyms

For the purposes of this document, the following acronyms are used:

- PO** - Legal person
- FO** - Natural person
- CP** - Certificate Policy
- CA** - Certification Authority
- OID** - Object Identifier
- PKI** - Public Key Infrastructure
- PMA** - Policy Management Authority
- CPS** - Certificate Practice Statement
- RA** - Registration Authority
- EFTA** - European Free Trade Association
- CRL** - Certification Revocation List
- HSM** - Hardware Security Modul

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	7 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public


NBÚ - Národný bezpečnostný úrad (National Security Office of Slovak republic)

CMA - Certificate Management Authority

IČO - Organisation identification number

SC - System certificate

QC - Qualified certificate

 NFQES BRAIN:IT	Version:	1.0
	Page:	8 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

1 Introduction

This document defines the rules for the performance of certification activities (hereinafter referred to as "Rules" or "CPS") for the NFQES CA Registration Authority (hereinafter referred to as "RA"). The Rules are based on the NFQES CA CP (OID=1.3.158.52577465.0.0.0.1.3.2), which apply to the implementation of a Public Key Infrastructure ("PKI") consisting of products and services that provide and manage certificates according to the X.509 standard for public key cryptography.

Certificates issued to end-users shall uniquely identify the entity to which the certificate is issued and bind that entity to the relevant key pair. Unless the document explicitly states that it refers to the certificate of the root CA or subordinate CA, the word certificate means the certificate of the end-entity.

The basic framework for the provision of qualified trust services consists of:

- Act No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amendment and supplementation of certain acts (Act on trust services)
- 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/EC (hereinafter also referred to as the "eIDAS Regulation")
- Decree of the National Security Authority (NBÚ) No 62/2014 Coll. amending Decree of the NBÚ No 133/2009 Coll. on the content and scope of operational documentation maintained by a certification authority and on security rules and rules for the performance of certification activities
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
- ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
- Act No 18/2018 on the protection of personal data, as amended


In the event of a difference between the Slovak and English versions of the Certification Policies and Certification Policy statements, or Rules for NFQES CA, the provisions set out in the Slovak version shall apply.

1.1 Overview

This document presents the rules for the performance of certification activities based on which the NFQES CA is established and operated by brainit.sk, s. r. o., (hereinafter referred to as the "Provider") and describes the activities of the external RA.

The Rules have been created in accordance with the NBÚ Decree No. 62/2014 Coll. and based on the materials Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647) and Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280).

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAINIT	Version:	1.0
	Page:	9 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

These policies define the creation and management of X.509 public key certificates for their appropriate use.

1.2 Title and identification of the document

Document version: 1.0

Date of effect: 1.4.2022

Description of the object identifier used (OID):

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** unique company identifier brainit.sk s.r.o. (IČO)
- **0.0.0.1** NFQES CA
- **9** The document „Policy of certification activities for NFQES CA – External Registration authority“
- **1** major version of the document

These rules apply to all certificates by means of which the Provider provides the following qualified trust services:

- A qualified trust service for the production and verification of qualified certificates for electronic signatures, where the private key is stored in a qualified electronic signature/seal creation device (QSCD)
- Qualified trusted service for the production and verification of qualified certificates for an electronic seal, where the private key is stored in a qualified electronic signature/seal creation device (QSCD)
- Qualified trusted service for issuing and verifying qualified certificates for web site authentication
- Qualified trusted service for storing qualified electronic signatures
- Qualified trust service for the storage of qualified electronic seals
- Qualified trust service for the creation and verification of qualified electronic time stamps


Provider's CA for the provision of qualified trust services:

Provider's Certification Authority	Certificate Serial Number	Issuer
NFQES CA	01	self-signed
NFQES ACA	4a2a267827944e5 323683482e7d5a7 2205491ac1	NFQES CA

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

- Certification Authority Certificate
- Certificate for the confirmation of the existence and validity of the certificate (OCSP)

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	10 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

1.3 PKI participants

This chapter describes the identity of the entities that perform tasks in the provision of trusted QC issuance and authentication services (hereafter referred to as QC services). The participants in the PKI are the entities referred to in this section.

1.3.1 Certification Authority

CA is an entity that provides qualified trust services as referred to in chapter **Error! Reference source not found.**

The CA is part of the hierarchical PKI structure in the issued qualified certificates (QC issuer).

Provider Certification Authorities are:

- Certification authority NFQES CA (serial number: 01), which issues qualified certificates to users and is not part of any hierarchical PKI structure (Self-signed certificate).
- Certification authority (intermediate CA) NFQES ACA (serial number: 4a2a267827944e5323683482e7d5a72205491ac1), which issues advanced certificates to users and is part of a hierarchical PKI structure (publisher).

A CA is an entity authorized by the PMA to create, sign, and issue public-key certificates for NFQES root CAs and end-user certificates.

The CA is responsible for all aspects of the issuance and management of the certificates, including control over the enrollment process, the identification and authentication process, the certificate creation process, the certificate publication process, and the certificate revocation process. The CA shall ensure that all aspects of its services and operations and the infrastructure associated with certificates issued under these rules are carried out in accordance with their requirements and provisions.

1.3.2 Registration Authority

An RA is an entity that acts under an RA contract on behalf of a Provider, performing selected activities and arranging for their provision to Customers/Applicants/Recipients in accordance with the NFQES CA CP, the NFQES ACA CP, and these rules, as amended from time to time.


The RA must conduct its activities in accordance with the approved version of the NFQES CA CP, the NFQES ACA CP, and these rules, as amended.

The components of the NFQES CA that are discussed in detail in these rules are:

- **Commercial RA** – which is intended for the provision of selected qualified trust services of the Provider to the public and is operated by a third party, based on a written RA contract with the Provider. This RA is a separate legal entity.
- **Corporate RA** – which is intended for the mediation of selected qualified trust services exclusively for the own needs of a specific PO or for the needs of the systems operated by it requiring the use of KC and is operated, based on a written contract on RA with the Provider, by a specific PO. Such RA is a separate legal entity.

If RAs are created under a written RA contract with a business associate and the business associate will operate its own RA, separate rules will be issued for that type of RA, which must

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	11 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

meet the minimum requirements defined by the Provider in the CP NFQES CA and the CP NFQES ACA in the current version.

The common term for CAs and RAs is Certificate Management Authority (CMA). The term CMA will be used when a function can be assigned to either a CA or an RA, or when the request is for both a CA and an RA.

1.3.3 End users

Certificate applicants and certificate holders

Certificate applicant means a natural person (FO) or legal entity (PO) that is authorized to apply for a certificate on behalf of an entity whose name may appear as an entity on the certificate.

An entity whose name may appear as an entity in a certificate may be:

- Natural person,
- Legal entity,
- component or system.

The applicant for a certificate becomes the Holder of that certificate upon acceptance of the certificate. The conditions that must be met by the applicant for an NFQES CA certificate are defined in the CP NFQES CA or CP NFQES ACA, as applicable.

A Certificate Holder is defined as an FO or PO that agrees to use the corresponding private key and certificate in accordance with the NFQES CA CP or NFQES ACA CP, as applicable, and these rules.

Customer means the PO or FO to whom the Provider provides trust services under an agreed Trust Services Agreement and that person pays for the services in question.

QC Holder means 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. The Certificate Holder in case it is an electronic signature is the signer.


A QC Holder may be:

- natural person,
- natural person identified in connection with legal entity,
- legal entity, which may be an organization or a unit or department thereof,
- a facility or system operated by or on behalf of the natural person or legal entity.

If the Customer is an FO and only his/her name and surname are indicated as the subject, the Customer and the Holder of the QC are the same FO, i.e. in case of non-fulfilment of the obligations imposed on both the Customer and the Holder, this FO is directly liable.

If the Customer acts on behalf of one or more Holders with whom it is connected (e.g. the Customer is a PO requesting the issuance of QC for its employees), the different responsibilities of the Customer and the Holder are defined in the document "General Terms and Conditions for the Provision and Use of the Trusted Service for the Issuance and

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	12 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Verification of Certificates" (hereinafter referred to as the "General Terms and Conditions") published on the Provider's website.

<https://nfqes.com/documents>

The following rules define the conditions to be met by the QC Holder and the Customer.

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

1. When applying for QC FO (Holder) is the Customer
 - the FO itself,
 - PO authorized to represent the FO (Holder), or
 - any entity with which the FO (Holder) is associated.
2. When applying for a QC for a PO, the Customer is
 - Any entity that is authorized under the relevant legal system to represent the PO, or
 - The statutory body of the PO applying on behalf of its subsidiaries or units or departments.
3. When applying for a QC for a facility or system operated by an FO or PO, the Customer is:
 - The FO or PO operating the facility or system,
 - the statutory body of the PO applying on behalf of its subsidiaries or units or departments.

1.3.4 Relying parties

A relying party is an FO or PO that relies on the trusted services of the Provider to act.

A relying party is an entity that, by using another's certificate to verify the integrity of an electronically signed message or to establish secure communications with the Certificate Holder, relies on the validity of the Certificate Holder's association with that public key. The party relying on the certificate should use the information from the certificate to determine the suitability of the certificate for a given use.


A synonym for the term Certificate Relying Party is the term Certificate User. This act based on trust in the certificate and/or on the basis of an electronic signature authenticated by the certificate.

1.3.5 Other parties

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

- overseeing the development and updating of the CP and CPS, including the evaluation of changes and plans for implementing the changes adopted,
- reviewing the results of audits to determine whether the Provider is responsibly complying with the provisions of issued CPs and CPSs,
- directing and managing the activities of both the Provider and the RA,
- interpreting the provisions of the issued CP and CPS and its instructions to the Provider and RA,
- reviewing the CPS to ensure that the Provider's practice complies with the relevant CP,

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	13 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- making recommendations to the Provider regarding corrective and other appropriate action,
- performing the function of internal auditor, delegating this activity to a separate staff member.

The PMA shall be the top-level decision maker, subject to final approval by the organization's management, on all matters and aspects relating to the Provider and its activities.

1.4 Use of the certificates

- **A QC made for a natural person**, where the private key is in the 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 person**, where the private key is contained in a QSCD is made for the purpose of supporting a qualified electronic seal within the meaning of Article 3(27) of the eIDAS Regulation.
- **A QC made for the authentication of a website** is made for the purpose of supporting the authentication of a website within the meaning of Article 3(38) and Article 45 of the eIDAS Regulation.
- **A QC made for an FO or PO**, where the private key is located on an HSM device (possibly a remote HSM) for the purpose of supporting a qualified electronic signature/seal.

1.4.1 *Appropriate use of certificates*

Certificates issued under the CP NFQES CA, the CP NFQES ACA, and this CPS are issued for the purpose of identifying the Holder of the Key Pair and Certificate within the PKI structure.

The cryptographic key pair (private and public) and the certificate issued by the Provider may generally be used in the usual manner, solely in accordance with their intended use, depending on the certificate, for the needs:

The Provider issues the following types of certificates to End Users pursuant to the CP NFQES CA and the CP NFQES ACA and these Rules:

- certificates for FOs intended mainly for the needs of securing electronic mail or signing electronic documents,
- certificates for POs intended for making electronic seals,
- mandate certificates for electronic signature issued by FOs,
- TLS certificates intended for web site authentication needs.

1.4.2 *Basic use of certificates*


No provisions.

1.5 Contact information

Founder, operator and owner of NFQES CA

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

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	14 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Registered office address: Veľký Diel 3323, 010 08 Žilina

ID (IČO): 52577465

TAX ID (DIČ): 2121068763

VAT ID (IČ DPH): SK2121068763

Mobile: +421 918 022 030

E-mail: info@brainit.sk

Provider's website: <https://nfqes.com/>

Trust Services website: <https://zone.nfqes.com/>

External registration authority

All provisions defined herein shall apply to all RAs unless otherwise agreed in a supplemental agreement.

1.6 Policy governance

1.6.1 Organization responsible for policy governance

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

Registered office: Veľký Diel 3323, 010 08 Žilina

ID (IČO): 52577465

TAX ID (DIČ): 2121068763

VAT ID (IČ DPH): SK2121068763

Register: Commercial Register of Distinct Court of Žilina, Section Sro, Insert No. 72902/L

1.6.2 Contact

Mobile: +421 918 022 030

E-mail: info@brainit.sk

Provider's website: <https://nfqes.com/>

Trust Services website: <https://zone.nfqes.com/>


1.6.3 Supervisory authority

Contact for Certificate revocation request:

Mobile: +421 918 022 030

E-mail: info@nfqes.sk

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAINIT	Version:	1.0
	Page:	15 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

2 General provisions

2.1 Obligations

2.1.1 Duties of the RA

RAs established by brainit.sk performing activities on behalf of the NFQES CA provide the mailroom function for the NFQES CA - specifically collecting and verifying information from customers - Certificate Applicants to be included in certificates. Direct contact between customers and the NFQES CA is made at the RA.


The RA receives applications for certificates, verifies and identifies the identity of Certificate Applicants, delivers issued certificates to their Holders or their authorized entities, arranges for the delivery of certificates and Certificate Revocation Lists (CRLs) to customers, receives and handles their complaints and grievances, collects from customers the established fees for CA services. In its activities, the RA shall be governed by the following rules.

The RA is responsible for ensuring that the information it collects has been verified by the RA and, therefore, that the information is correct at the time.

RA staff are required to:

- follow the provisions of the NFQES CA CP, NFQES ACA CP, associated policies, and these rules, as well as PMA guidelines,
- keep the RA's private key confidential - immediately report to the NFQES CA if your private key is compromised, if you lose your smart card, or if you forget the password to access your private key,
- retain RA office correspondence conducted in written or electronic form and send written documents to the CA for archiving as directed,
- keep a record of RA activity in a record book,
- record in the record book all other events at the RA, in particular events relating to the RA private key (its compromise, receipt or loss of a smart card, forgetting the password for access to the private key), RA workplace security, receipt (and how it is handled) of a complaint, comment or request for interpretation of the CP and CPS,
- email communication between the RA and CA to be carried out using only signed documents and, where appropriate, password encryption of documents,
- to carry out the registration of customers - Certificate Applicants, to verify their identity, the values of the distinguished name items contained in the certificate application, the format of the certificate application, to collect documents used in the registration process that do not comply with the provisions of this document, to reject them,
- forward the received certificate requests for processing by entering them together with the necessary data into the NFQES CA information system (IS) or by personal delivery to the Provider's place of performance,
- be responsible for verifying that the information she has collected is correct at the time,

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	16 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- receive, log, and refer for processing suggestions, comments, or requests for interpretation of the CP and CPS and, if their resolution is not clear from this document or other instructions binding on the RA, refer them to the NFQES CA for processing,
- receive requests for certificate revocation - refer eligible requests for processing, deny others,
- collect from customers the fees set forth for the services provided by the NFQES CA.

The RA shall be entitled to suspend its activities for an indispensable period for urgent technical or operational reasons. It shall report this fact to the NFQES CA without delay.

An RA performing the registration functions described in this policy shall comply with and act in accordance with the provisions of the CP NFQES CA, the CP NFQES ACA, and the provisions of this document. If an RA is found not to be following these obligations, appropriate action will be taken against the RA, including suspension as an RA.


2.1.2 Obligations of the certificate Holder

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

- provide true, accurate, and complete information to the Provider when applying for a certificate as required by this CPS, the CP NFQES CA, or the CP NFQES ACA, as applicable,
- use the QC in accordance with the limitations set forth in the General Conditions,
- protect their private keys in accordance with these Rules, the General Conditions, the CP NFQES CA, or the CP NFQES ACA, as applicable,
- use the private key only after receiving a QC for the public key with which it forms a pair (in the case of QSCD devices),
- in the case of a QC that has not yet expired, immediately notify the Provider if it suspects that:
 - its private key has been lost, stolen or compromised,
 - has lost control of his/her private key by compromising his/her login credentials (password or OCRA token),
 - inaccuracies or changes in the contents of the certificate,
 - immediately request revocation of the QC if any of the information provided in the QC subject 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 their Private Key and QC such as ceasing to use the Private Key upon expiration or cancellation of the QC,
- to use the QCs provided only for the relevant purposes,
- immediately discontinue use of the private key upon its compromise,

The obligations of the QC Holder also apply to the FO or PO that has taken over certificates for the components, systems or websites it manages.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	17 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

2.1.3 Obligations of the relying parties

Relying parties are obligated to:

- use the QC only for the purpose for which it was issued,
- verify each QC for validity before relying on the QC (i.e. verify that the QC is valid at that time and that it is not on a CRL issued by the Provider),
- 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 QC,
- 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.

2.2 Legal warranties

The Provider, through these Rules, the CP NFQES CA or CP NFQES ACA, as applicable, and the Service Agreement, as well as the Certificate Issuance Agreement, expresses the legal prerequisites for the use of the issued QCs by their Holders and Relying Parties.

2.2.1 Provider declarations and warranties – NFQES CA


No warranties or representations are given by the Provider in respect of the trust services provided, except as set out in the relevant CPs and related CPSs.

The Provider reserves the right, if it deems it appropriate, to amend its CPs and these rules, at its sole discretion or in accordance with applicable legislation.

To the extent specified in the individual sections of the CP NFQES CA or CP NFQES ACA or CPS issued, as applicable, the Provider declares:

- compliance with its obligations under these rules, as well as other published procedures and policies, including the CP NFQES CA and CP NFQES ACA and their associated CPSs,
- complying with its obligations under the eIDAS Regulation and applicable national legislation,
- promptly notifying affected entities in the event of compromise of their private keys in accordance with the CP NFQES CA and CP NFQES ACA and this policy,
- putting in place security mechanisms, including those for private key generation and protection, relating to the protection of its PKI structure,
- the availability of a hard copy or electronic version of these rules and other published policies online,
- the fact that the Holder becomes or is the owner of the private key at the time the QC is executed within the meaning of the CP NFQES CA, the CP NFQES ACA, and this policy,

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	18 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- the accuracy of the information contained in the executed QCs to the best of the Provider's knowledge and the compliance of the issued QCs with the requirements of the eIDAS Regulation,
- compliance with data protection regulations in the handling of Holders' personal data.

2.2.2 RA declarations and warranties

All Provider's external RAs must provide trust services under a contractual relationship with the Provider and in accordance with the CP NFQES CA, CP NFQES ACA, and these rules. See further the provisions in Section 2.2.

2.2.3 Declarations and warranties of participants

Except as otherwise provided in these Rules or in the applicable agreement with the Holder/Customer, the Holder is solely responsible for:

- providing accurate and correct information in communications with the Provider,
- reading and agreeing to all the terms and conditions given in the CP NFQES CA or CP NFQES ACA, as applicable, the applicable CPS to the CP, and these Rules, which are available in the Provider's repository (see Section 1),
- use the issued QCs only for appropriate purposes in accordance with the CP NFQES CA, the CP NFQES ACA, as applicable, the applicable CPS to the CP, and these rules,
- discontinuing the use of QCs if any information in them is found to be misleading, outdated, or incorrect,
- use its best efforts to prevent the compromise, loss, declassification, modification, or any unauthorized use of the private key corresponding to the public key contained in the CP issued by the Provider.

2.2.4 Declarations and warranties of the relying parties

The declarations and warranties of the relying parties are part of the General Terms and Conditions for the provision and use of the Provider's trusted service for the production and verification of certificates, which are available on the Provider's website.

2.2.5 Declarations and warranties of other participants

No provisions.

2.3 Financial responsibility

2.3.1 Insurance cover

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


2.3.2 Other assets

No provisions.

2.3.3 Insurance or guarantee for end-users

No provisions.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	19 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

2.4 Arbitration and dispute resolution

2.4.1 Dispute resolution provisions

The Holder/Customer has the right to send the Provider a complaint, suggestion or claim about the 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 RA is authorized to receive and handle simple complaints, claims and inquiries from Applicants or Certificate Holders unless there is a reason to refer them to the NFQES CA.

The RA Courts 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, he/she is entitled to contact the out-of-court dispute resolution entity, which is the Slovak Trade Inspection, or another PO registered in the list of entities for alternative dispute resolution of consumer disputes maintained by the Ministry of Economy of the Slovak Republic. The Holder/Customer has the right to choose which of the above-mentioned alternative dispute resolution entities to contact. Before proceeding to judicial or out-of-court dispute resolution, the parties are obliged to first try to resolve the dispute by mutual agreement.

2.4.2 Governing 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 General Terms and Conditions and these Rules 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 legislation of the Slovak Republic.

2.5 Fees

The Provider is obliged to publish in an appropriate manner (via its website) the valid price list of its trust services or information under which contractual conditions it is possible to obtain trust services.


2.6 Disclosure and storage

2.6.1 Disclosure of CA information

The storage must be located to be accessible to QC Holders and Cooperating Parties and in accordance with the overall security requirements set forth in the CP NFQES CA and CP NFQES ACA, as applicable.

The Web site shall serve as the Provider's repository. The exact URL address is set forth in Section 1.5 of this document. The Provider's website is publicly accessible via the Internet to QC Holders, Relying Parties, and the public at large.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	20 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

The publicly available information contained on the Provider's website is of a controlled access nature.

The Provider publishes, online via its website, information that is accessible to Customers, QC Holders and Related Parties at least to the extent that:

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

The Provider shall publish these rules, as well as other documents related to the provision of trust services under this document, in an on-line mode via its website.

The Provider shall not disclose information on issued certificates which are issued for the internal needs of the contractual partners, and it is contractually agreed with the partner not to disclose them.

2.6.2 Frequency of publication of information

The Certificate revocation list (CRL) must be published as follows:

CRL Publisher	Publishing frequency	nextUpdate thisUpdate interval
CA NFQES	12 hours	24 hours

Information about the cancelled CRL shall be available on the Provider's web site that serves as its repository. The CP and CPS, or revisions thereto, must be posted as soon as possible after their approval and issuance. All other information to be published in the repository must be published as soon as practicable.

A certificate shall be published immediately after its issue and shall be immediately available for download by the Certificate Holder. Information about the issued certificate can be found on the Provider's website, which serves as the repository of the NFQES CA.

2.6.3 Access controls

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

2.6.4 Storage


See sections 2.6.1 and 2.6.3.

2.7 Compliance audit

2.7.1 Frequency of compliance audit for a given entity

The Provider shall undergo a compliance audit at least every 24 months in accordance with the requirements of the trust services it provides.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	21 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

2.7.2 Auditor identity and qualification requirements

The Conformity Assessment Body and its audit delegates must be competent in the field of conformity audits, meet 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" version 2.2.2 as a minimum, in accordance with the NSA certification scheme that governs the requirements of the ETSI standard, and be thoroughly familiar with the CP NFQES CA, the CP NFQES ACA, the relevant CPSs, and this document.

2.7.3 Topics covered by the compliance audit


The purpose of the audit is to confirm that the Provider has a satisfactory system of RA work that guarantees the quality of services provided by the NFQES CA and that guarantees that the RA is acting in accordance with all requirements of this policy. The subject of the compliance audit shall be all aspects of the NFQES CA's operations related to these rules.

2.7.4 Actions taken to correct deficiencies

When the auditor identifies a discrepancy between the operation of the external RA and the applicable requirements or provisions of the CP, the issued CPS, and this document, the following actions must be taken:

- the auditor identifies and records the discrepancy,
 - The auditor shall identify and document exactly where the discrepancy lies between the actual operation of the external RA and the requirements of the CP, the CPS or the provisions of this document.
- the auditor must notify all stakeholders of the discrepancy,
 - the auditor shall report the discrepancy to the appropriate responsible persons, which may be managers or executives of the external RA who are responsible for ensuring compliance with the CP, the CPS, and this document, as well as the NFQES CA.
- The NFQES CA will propose a PMA,
 - the PMA must identify an appropriate corrective action, including the expected time required to implement it (may be feasible in conjunction with the auditor).
- monitoring the implementation of corrective actions
 - the designated person (responsible person for the external RA as well as the NFQES CA) monitors whether the external RA has implemented the proposed corrective action within a reasonable timeframe and whether the discrepancy has been resolved.
- recording of progress and results
 - all actions, measures, and results are recorded in a report or documentation that includes how the discrepancy was resolved and whether full compliance was ensured.
- re-audit

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	22 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- if the discrepancy has not been adequately resolved or if continued compliance with the requirements needs to be verified, a re-audit or follow-up may be scheduled to assess whether all deficiencies have been corrected.

2.7.5 Handling of audit results

The Conformity Assessment Body must submit the results of the audit in written or electronic form to the auditee (NFQES CA or external RA), who must implement and take necessary corrective action based on the results.

Within three business days of receipt, the Provider or External RA must submit the resulting Conformity Assessment Report to the supervisory authority.

The implementation of the corrective measures shall be brought to the attention of the competent authority. A specific compliance audit or a partial compliance audit focusing on a given aspect of the audited entity's activities may be requested to confirm the implementation and effectiveness of the corrective measures.

2.8 Secrecy

2.8.1 Types of protected information

All information subject to appropriate protection is contained in the CP NFQES CA, CP NFQES ACA, and private keys belonging to the NFQES CA and external RA components.

Confidential information subject to appropriate protection is:

- internal infrastructure (e.g. documents, policies, directives, workflows, files, scripts, passwords, pass phrases, etc.) used for the Provider's operation, including its RA, the Provider's private keys used for signing executed QCs,
- the OCSF responder's private keys used to sign responses to requests to confirm the existence and validity of QCs,
- 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 by the Customer or the Provider as "Internal" or "Confidential". Confidential information may include, but is not limited to, data, specifications, analyses, commercial information, know-how, documentation, procedures, processes, information relating to clients or business partners or other information from the Provider's or its Customers' IS in any form.

All confidential information shall be treated as sensitive information and access to it shall be limited to those persons who strictly need the information to perform their job duties.

2.8.2 Circumstances of release of confidential information

Neither NFQES CA nor any external RA shall disclose any information regarding the Certificate Applicant or Certificate Holder to any third party (unless otherwise defined in the General Terms and Conditions or the Personal Data Processing Rules), unless the information is considered public or is required by law or by order of a competent public authority, such as

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	23 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

the police, court, prosecutor's office, or is the subject of a contract between the Provider and its partner.


Any request for the release of information that is not considered public shall be authenticated and properly documented.

The Provider treats the personal data of the Customer in accordance with the applicable laws of the Slovak Republic and does not disclose them to any third party, except to entities that have the right to control the Provider's activities and except as defined in the General Terms and Conditions and the Rules for the Processing of Personal Data.

2.9 Intellectual property rights

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

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	24 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

3 Identification and authentication

3.1 Initial registration

3.1.1 Types of names

Each CA can create certificates that contain X.500 Distinguished Names (X.500 Distinguished Name, hereafter referred to as "Distinguished Name"), specifically in accordance with X.501 and X.520 respectively, and names in accordance with RFC5322 Internet Message Format.

Customers must choose themselves the Distinguished Name to be included in their QC.

3.1.2 The need for meaningful names

The term "meaningfulness" means that the form of the name takes a commonly used form to establish the identity of the Holder (FO, PO, public authority - OVM, website). The names used must reliably identify the persons to whom they are assigned.

In some cases, accented characters are not used in the content of the QC, and these are replaced by equivalent ASCII character table characters (e.g. 'á' is replaced by 'a'; 'č' is replaced by 'c', etc.). Such a case may be requested by the customer when the equipment on which the QC will be used is dedicated HW that cannot be replaced (or is not cost-effective for the customer) and does not support the UTF-8-character set.

3.1.3 Uniqueness of names

The provider is responsible for the uniqueness of names across the QC holder community.

3.1.4 Dispute resolution procedure for name clashes

The interpretation of the various forms of names in the QCs produced by the Provider must be consistent with the QC profiles described in the CP NFQES CA in Section 7 or the CP NFQES ACA, as applicable.

3.1.5 Recognition, authentication and the role 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/Recipient may be used in the QC. No other authentication of the Provider's trademarks shall be made.

Provider shall not knowingly issue a QC containing a name that has been determined by a court of competent jurisdiction to infringe the trademark of another. Provider shall have no obligation to investigate trademarks or resolve trademark disputes.

3.1.6 Proving private key ownership

The key pair for which the QC for the electronic signature intended for the execution of the qualified electronic signature or the QC for the electronic seal intended for the execution of the qualified electronic seal must be generated directly in the device for the execution of the qualified electronic signature or the seal, which meets the requirements set out in Annex II of the eIDAS Regulation (hereinafter referred to as "QSCD"). In the case of remote certificates, these QCs shall be generated directly on the secure HSM hardware device.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	25 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

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

3.1.7 Authentication of the identity of the legal entity (organization)

An applicant for a certificate acting on behalf of a PO must submit the name of the PO, other identification data, if any (usually e.g. a registration number), address and proof of the existence of the PO in the form of an extract from the commercial register not older than 3 months.

The RA verifies these data and verifies, in addition to the identity of the authorised user (applicant), that the person has the right to act on behalf of the PO in respect of the certificate in question. Detailed provisions for the submission of identification documents are defined in the CP/CPS NFQES CA or CP/CPS NFQES ACA, as appropriate.


Verification of the identity of the PO is carried out at the seat of the external RA or also outside the seat of the RA in the presence of a responsible employee of the external RA (trip to the customer) in the physical presence of the statutory body authorized to act for the company also by means of at least two valid identification documents of 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 will bring an extract from the Commercial Register applicable for legal transactions not older than 3 months (there is a possibility to verify the existence of the PO also by the RA employee, through the slovensko.sk portal and by requesting an extract from the Commercial Register directly by the RA employee), the statutory body authorized to act for the company will personally sign and agree to the General Terms and Conditions, and the statutory body authorized to act for the company will sign the application for the issuance of the certificate. The external RA officer shall assess the validity and authenticity of the identification documents (checking the various security features of the documents) and retain copies of those documents provided. Should the external RA worker find anything objectionable about the documents, he/she must reject them. He/she shall then check whether the data from the extract from the Commercial Register applicable for legal transactions and the data provided on the identification documents match the data provided in the Provider's IS and in the application for the certificate. If the information in the IS and the application for the certificate match the information on the identification documents and on the extract from the Commercial Register, the PO is verified.

The identification documents of a member of the statutory body must contain at least the following:

- first and last name,
- address of permanent residence,
- birth number or date of birth.

In the case of non-business entities such as a civil association, municipality, church, foundation, etc., such PO must demonstrate, in addition to its identity, the legality or "reason"

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	26 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

for its existence, using and referring to the law or other regulation that refers to the entity of the type in question, the deed of incorporation, etc.

3.1.8 Authentication of the identity of a natural person

The FO may be an adult citizen of the Slovak Republic or a foreign national.

Verification of the identity of the FO is carried out at the seat of the external RA or also outside the seat of the RA in the presence of a responsible employee of the external RA (trip to the customer) in the physical presence of the person, also using at least two valid identification documents, at least one of which must be an official document with the likeness of the face, the so-called face-to-face identification. In this case, the FO shall personally sign and agree to the General Terms and Conditions and the FO shall sign the application for the issuance of the certificate. The RA officer will assess the validity and authenticity of the identification documents (checking the various security features of the documents) and keep copies of these documents provided. Should the external RA worker find anything objectionable about the documents, he/she must reject them. He/she shall then check that the data provided on the identification documents match the data provided in the Provider's IS and in the application for the certificate. If the data in the IS and the certificate application match the data on the identification documents, the FO shall be deemed to be authenticated.

At a minimum, FO identification documents must include:

- first and last name,
- address of permanent residence,
- birth number or date of birth.


If the FO represents another FO, he/she must additionally prove that he/she has been authorized by the authorizing FO to act on his/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 (PPA), the Customer must present the authorization to act on behalf of the represented person in the form of:

- a document proving that the person in question is a statutory body of the given PO or OVM,
- a letter of authorization, if the FO is an employee of the PO on whose behalf he acts and is in an employment or similar employment relationship with it,
- a power of attorney certified by a notary public, if the FO in question 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 function, the Customer must prove in a credible manner that he/she is an OVM, that he/she 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's web site.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	27 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

3.1.9 Device, system or website 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.

Therefore, the QC of the web site must be formally assigned to the FO acting on behalf of the PO (organization) that has demonstrable control over the web site for which the QC is made. All the conditions in sections 3.1.7 and 3.1.8 in this document apply, as well as the additional conditions set out in this section.

The FO is required to provide the Provider with the following information:

- system/device public keys (contained in the QC application),
- identification of the system/device,
- the authorization of the system/device and its attributes (if any to be included in the QC),
- contact details to enable the Provider to communicate with the FO if necessary.

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

Methods for performing this data control and authentication include:

- verification of the identity of the FO in accordance with the requirements of section 3.1.8,
- or verification of the identity of the PO to which the component/system belongs, in accordance with the requirements of section 3.1.7,
- verification of the legitimacy of the use of the data to be included in the individual QC entries, with emphasis on the content of the commonName (CN) entry.


Note: The typical value of this item is a well-defined domain name (FQDN).

In the case of the use of a domain name, it is a requirement that the relevant second level domain and above is under the control of the Customer requesting the KC for the authentication of the website.

Verification that the Customer is the owner of or has control over the domain whose FQDN is or will be listed in the Subject Alternative Name (SAN) field 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 this 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.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	28 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- 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 Customer's request for the issuance of a TLS/SSL certificate.

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 the name of the PO, trademark, trade name, address, location, or other text indicating an identifiable FO or PO, without reliably verifying this information.

Checking the particulars on the documents

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

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

3.1.10 Identity authentication with contractors

Authentication of the identity of the FO or the component with the Provider's contractual partners (business partners) is carried out in cooperation with the responsible persons of this company.

Some procedures are simplified in this case and do not have to be performed, e.g. verification of domain ownership, verification of e-mail account control, etc.

3.1.11 Documents to be presented

All documents submitted to the RA by applicants for services must be either originals or certified copies of originals. They must not contain any additions, alterations, crossings out, etc. Documents bearing an expiry date must be valid.


If the RA has doubts as to the identity of a potential customer (e.g. an apparent discrepancy between the photograph in the identity document presented and the customer's appearance, a discrepancy between two documents presented, etc.), he may refuse to register the customer.

Any documents submitted in a foreign language (other than Czech) must be translated into Slovak by an official translator - an expert.

At the request of a potential customer or RA, any disputes in proving identity shall be resolved in accordance with the procedure set out in section 2.4.

When submitting the documents, it is required that the RA branch must be presented with the originals of these documents for inspection and copies of the originals (they do not have to be certified), except for personal documents identifying the identity of the applicant or authorized person, which are used for archiving for the needs of the CA. Submission by the applicant of an extract from the commercial register or the trade register obtained from the Internet is not sufficient, as it is only of an informative nature and is not usable for legal acts.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	29 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Natural person

The FO submits two documents identifying him/her.

The primary document is:

- citizen of the Slovak Republic – valid ID card or passport
- a foreign national – an identity card, i.e. an identification card, a residence permit for the territory of the Slovak Republic, or a passport or a foreign card.

A secondary document may be:

- passport
- driving license
- health insurance card
- birth certificate
- military identity card or military booklet
- temporary residence permit (or permanent residence permit) in the case of a foreigner
- a firearms license issued by the competent police department
- service card
- other...

It is required that at least one of the documents submitted must be a document that includes a photograph of the person concerned (a photo with a likeness of his/her face).

In the case of an application for a certificate for the needs of the contractor or an application for its cancellation, it is sufficient for the FO to prove his/her identity with one of the following personal documents - ID card or passport. The applicant for a certificate issued for the needs of the contractual partner must also fulfil other conditions for the issue of a certificate of this type, which shall be determined by the contractual partner.

If the FO represents another FO in the RA, he/she must additionally present an officially certified (notarized) power of attorney, the text of which makes it clear that the representing FO has been authorized by the authorizing FO to act on its behalf in the matter in question.


If the applicant for the certificate is a legal representative (usually a parent), he/she must additionally submit the child's birth certificate, the adoptive parent must additionally submit a court decision or an extract from the registry office. The identity card in which the child is registered is also sufficient proof.

Natural person – employee

If the applicant for the certificate is an FO, which also has the name of the organisation mentioned in the application, it shall submit the documents according to the previous chapter (Natural person). At the same time, he/she must provide consent to the issuance of the certificate from the employer, for example by presenting a power of attorney for the act. If the applicant is an employee of the contractor, this requirement is replaced by the consent to issue from the contractually designated contact person.

Legal entity

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	30 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

In this case, the applicant for a certificate shall submit the documents listed in the chapter Legal entity. At the same time, he/she shall submit the documents referred to in section 3.1.7.

If several persons act jointly on behalf of the PO, it is necessary to submit a power of attorney certified (by a notary public), the text of which makes it clear that the representing FO has been authorized by the authorizing FOs to act on their behalf in the matter in question.

Device or system

See provisions in section 3.1.9 of this document.

All documents submitted to the RA by applicants for the Provider's services must be either originals or certified copies of originals. They must not contain any additions, alterations, strikethroughs, etc. Documents bearing an expiry date must be valid.

If the RA has doubts as to the identity of a potential customer (e.g. an apparent discrepancy between the photograph in the identity document presented and the customer's appearance, a discrepancy between two documents presented, etc.), he may refuse to register the customer.

Any documents submitted in a foreign language (other than Czech) must be translated into Slovak by an official translator - an expert.

At the request of a potential customer or RA, any disputed cases of proof of identity shall be resolved in accordance with the procedure set out in section 2.4 of this document.

When submitting the documents, the RA branch is required to present the originals of these documents for inspection or officially certified copies of the originals, except for personal documents identifying the identity of the applicant or the authorized person. To archiving these documents for the NFQES CA, it is appropriate to submit copies of these documents, but they no longer need to be certified. The applicant's translation of an extract from the commercial register or the trade register obtained from the Internet is not sufficient, as it is only informative and not usable for legal transactions.


3.1.12 Verification of data on documents submitted

In the event of any reasonable doubt as to the identity of a potential customer, RA may refuse to register the customer. In particular, the RA officer shall check the following on the documents submitted:

Personal documents of the FO:

- the validity of the document presented - in the case of an invalid identity document, the same procedure is followed as for a missing identity document - the RA will refuse registration
- the age of majority of the FO (i.e. 18 years of age) - the RA will refuse the registration of minors, while the legal representative (usually a parent) has the right to act for minors
- whether there is an obvious discrepancy between the photograph in the identity document and the appearance of the identity document holder - if so, the RA may refuse registration

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	31 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- the inconsistency of the documents submitted, i.e. whether the information on one document contradicts the information on another document
- security features on the documents submitted

Extracts from the commercial register:

- the statement is not older than 3 months
- whether the FOs (one FO is sufficient, unless otherwise indicated on the statement) who submitted the statement have the right to act (sign) for the PO (i.e. whether they are its statutory representatives)
- whether the extract is officially certified (by a notary or registry office), if it is not the original or not provided from the slovensko.sk portal

Power of attorney:

- whether the power of attorney is officially certified (by a notary or registry office)
- whether the information given in the power of attorney, which defines the representing FO or PO, corresponds to the information given in the personal documents of the representing FO or the information given in the extract from the commercial register of the representing PO
- the scope of the power of attorney - i.e. whether the power of attorney authorizes the authorized FO or PO to perform the required act on the RA on behalf of the authorizing FO or PO
- whether the power of attorney is not limited in time or, if it contains another condition, whether this is fulfilled

Honorary declarations:

- authorization to sign – whether the person signing the declaration is authorized to represent the PO. Eligibility is checked according to the extract from the ORSR or other register of legal entities. If the person signing is not listed in this extract, he/she must present another document based on which he/she can act for the company (usually a notarized power of attorney)

The type of documents submitted (e.g. ID card, passport) and the relevant data from them shall be recorded electronically in the IS of the Provider by the RA employee.


In case of detected deficiencies in the submitted documents or submission of incomplete documents, the RA officer must refuse the registration of the applicant. In this case, the certificate issuance service will be refused.

The RA must also accept documents submitted by the applicant in electronic form and signed with a valid QES (extract from the ORSR, power of attorney, declaration, authorization, etc.)

3.1.13 Initial registration of RA

The initial registration of a person in the RA role is performed under the same conditions described above as in the case of a customer - applicant for a personal certificate. The actual verification of the identity of the RA personnel shall be performed by the Provider's personnel unless another mechanism is contractually agreed.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	32 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

3.2 Issue 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 IS of the Provider.

The conditions for issuing a Subsequent Certificate are described in detail in the CP NFQES CA in Section 4.7 or the CP NFQES ACA, as applicable.

The RA shall issue a certificate without a personal visit of the Holder only in the case of a personal certificate or a system certificate for the PO after the conditions specified in section 3.2 of the current CP NFQES CA or CP NFQES ACA, as applicable, have been met.


3.3 Issuance of a subsequent certificate after revocation of the old one

Upon revocation of the certificate, the applicant for a subsequent certificate must comply with all the requirements of the initial registration.

3.4 Application for revocation of a certificate

The certificate revocation request must be authenticated, see section **Error! Reference source not found.** of this document. A certificate revocation request can be authenticated using the private key belonging to the certificate, whether the private key has been compromised.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	33 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

4 Operational requirements

4.1 Applying for a certificate

When an applicant applies for a certificate, the applicant and the RA must take the following steps:

- the RA must verify and record the identity of the applicant (as specified in section 3.1), as well as verify all other information contained in the certificate, using independent sources and alternative communication channels,
- the applicant shall demonstrate that the public key forms a key pair with the private key owned by the certificate applicant (as per the provisions in section 3.1.6),
- the applicant must provide sufficient supporting documentation to verify any identifying data to be contained in the certificate.

All communications between the CA components related to the certificate request and issuance process are to be authenticated and protected from modification by mechanisms appropriate to the requirements of the data to be protected using previously issued certificates.

4.1.1 Who can apply for a certificate

The Provider may be requested to issue:


- QC for electronic signature
 - FO or FO authorized by the Holder or by a person acting on behalf of the Holder by virtue of a law or a decision of a competent authority
- QC for electronic seal
 - any entity (the Customer) which is authorized to act on behalf of the PO in accordance with the applicable legislation of the Slovak Republic
- QC for website authentication
 - FO or PO operating the equipment or system
- Mandate certificate
 - FO authorized by or under the law to act for another person or OVM, or an FO who performs an activity pursuant to a special regulation (Section 8(1) of Act No. 272/2016 Coll.) or performs a function pursuant to a special regulation (Section 8(1) of Act No. 272/2016 Coll.).
 - any entity (Customer) with which the FO is associated, e.g. their employer, a non-profit organization of which they are a member, etc.

4.1.2 Procedure for obtaining a certificate

The Customer must take the following steps in preparation before visiting the Provider or the Provider's RA, as applicable:

- to familiarize themselves with the Provider's General Terms and Conditions and the Rules for the Protection of Personal Data Processing, which are available on the Provider's website,

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	34 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- to familiarize themselves with the Provider's relevant CPs (CP NFQES CA, CP NFQES ACA) and this document and, where applicable, the principles and guidelines for obtaining QC,
- Prepare the values for each item on the QC claim so that these values are consistent with this document and the applicable Provider CP,
- prepare the selected identity documents or other necessary documents,
- in the case of a mandate certificate, prepare the authorization to act on behalf of the represented person (declaration, authorization or notarized power of attorney or documents proving his/her function or activity or that he/she is an OVM), according to the list of authorizations published on the NSA's website,
- in the case of physical registration using an external RA or directly at the CA, arrange a date for a personal meeting.

Procedure prior to the issue of the QC:

Prior to issuing a QC, the employee representing the Provider or RA, as applicable, must:

- inform the FO present about the General Terms and Conditions and the Conditions of Processing of Personal Data
- verify the identity of the Holder/Customer or the person representing him/her according to the documents submitted and record all mandatory personal data in the IS of the Provider,
- make photocopies of the identity documents submitted,
- verify all other submitted documents according to the established procedures.

4.2 Issuance of the certificate

The Provider shall not create a QC until all verifications and changes, if any, have been completed to the satisfaction of the NFQES CA. The Provider shall not be responsible for any additional costs incurred by the Certificate Applicant during the registration process, e.g., due to the need to revisit an external RA, e.g., due to incomplete or missing documents or other deficiencies.

Although the Applicant prepares most of the QC data items, the responsibility remains with the external RA to verify that the information is correct. It is the responsibility of the External RA to verify the Applicant's data.


The Provider has the right not to issue a QC even though the QC Applicant has successfully passed the RA registration process, if a material fact is subsequently discovered that prevents the QC from being issued (e.g. an error in the format of the certificate application).

After sending the QC request from the external RA to the Provider's IS, the Provider must perform a verification of the received request to verify that:

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

If all the requirements for issuing a QC are met, the Provider shall issue the QC.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	35 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

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

The Provider may, at the Customer's request, execute the QC in the production environment to verify and test its functionality. In such a certificate, the distinguished name entries shall clearly indicate 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.

4.2.1 Delivery of the private key to the certificate Holder

The provisions defined in the CP NFQES CA, CP NFQES ACA apply.

4.2.2 Delivery of the CA public key to users

The CMA and the parties relying on the certificates must act in concert to ensure authenticated delivery of the certificate to the NFQES CA.

Acceptable methods to deliver and authenticate an NFQES CA or NFQES ACA certificate are:

- uploading the certificate from the NFQES CA IS,
- personal receipt of the certificate at an external RA or directly at the CA,
- making the use of the remote certificate available in the Provider's IS in case of a remote certificate.

4.3 Receipt of the certificate

Certificates are created and issued in an automated and continuous manner, the Applicant will usually be able to collect the issued certificate during the same visit to the external RA when he/she applied for the certificate. Immediately after the certificate has been issued, the certificate applicant will be able to collect their certificate.

The applicant for a certificate may have another FO or CA represent him/her at the external RA when collecting his/her certificate, under the same conditions as when applying for a certificate (see sections 3.1.7 or 3.1.8 of this document). Acceptance of the certificate will normally take place at the same RA where the application for the certificate was made.

Notification of certificate issuance will be sent to the email address on the certificate, or by telephone or notification in the Provider's IS, and delivered to the Certificate Holder or the entity that represents the Certificate Holder, along with the NFQES CA certificate.

4.4 Certificate suspension and certificate revocation


4.4.1 Certificate revocation

Circumstances of certificate revocation

A certificate must be revoked when the binding between the subject and its public key defined in the certificate is no longer considered valid. Examples of circumstances that break this binding are:

- the certificate holder or other authorized party requests revocation of the certificate,
- it is suspected that the private key (corresponding to the public key in the certificate) has been compromised or the certificate has been otherwise misused

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	36 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- the Certificate Holder is found not to be in compliance with its obligations as a Certificate Holder under the terms of the Certificate,
- the identifying information or appended elements of any names in the certificate become invalid,
- it is suspected that the Certificate has not been issued in accordance with the Provider's applicable CPs and these Rules or the corresponding CPS for RAs and CAs,
- any of the information in the certificate is found to be erroneous or incorrect,
- the Provider ceases to operate for any reason and does not contract with another CA to provide information on revoked certificates on behalf of the Provider,
- the circumstances that required the issuance of the certificate (testing, application verification, etc.) have ended,
- the private key has been lost,
- the technical parameters or format of the certificate could lead to an unacceptable risk from the point of view of software vendors or relying parties (change of cryptographic algorithms for signing, length of cryptographic keys, etc.),
- death of the Certificate Holder,
- compromise of the Provider's private key,
- a final judgment or interim measure of a court.

Whenever the CA becomes aware of any of the above circumstances, the certificate in question is revoked and inserted into the CRL. Revoked certificates shall appear in all new editions of the CRL, at least until the certificates in question expire.

Entities that can apply for certificate revocation

The Certificate Holder (or the FO or PO authorized by him/her) may at any time request, in the manner set forth herein and in the General Terms and Conditions, the revocation of his/her own Certificate, even without giving any reason for the request for revocation of his/her Certificate.


The RA shall make a proposal to the NFQES CA for revocation of the Certificate Holder's Certificate if it becomes aware that any of the circumstances listed above have occurred.

If the certificate was issued to an employee of the contractor, it may be agreed in the relevant contract who, other than the Certificate Holder, has the right to request revocation of the certificate, in what manner and under what circumstances.

The Certificate Holder may also request the revocation of the Certificate:

- CMA - the employee in question is required to document this fact, including the reason for his or her action,
- entity (FO or PO) based on inheritance proceedings (the Provider must attach to the documents on revocation of the certificate a copy of the documents which show the right of the entity to request revocation of the certificate),
- a court through its judgment or interim measure (the Provider must attach a copy of the relevant court decision to the documents on revocation of the certificate),

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	37 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- a person authorized by the court (the Provider must attach a copy of the relevant court decision to the revocation documents).
- OVM or a person with whom the mandator performed an activity according to a special regulation (§8 (1) of Act No. 272/2016 Coll.) or a function according to a special regulation (§8 (1) of Act No. 272/2016 Coll.), the principal or the mandator.

In the case of an RA certificate, in addition to the Certificate Holder (the RA), the PMA may also request revocation of the certificate if a compelling circumstance (see Circumstances for Revocation of a Certificate) is found to justify revocation of the certificate.

Procedure for requesting the revocation of a certificate

The request for certificate revocation can be submitted electronically using the IS of the Provider or directly to the CA. Certificate revocation must be authenticated using 2FA in the IS of the Provider, in case of a personal visit to the CA/RA, identification documents (OP, passport, other...) must be presented. The RA must inform the Certificate Holder of the certificate revocation after the revocation.

A request for certificate revocation can also be made by an authorized person in person to the RA or directly to the CA through the same authentication process as required for the initial registration of the Holder/Customer.

To prevent arbitrary certificate revocation by an unauthorized party, authentication of the certificate revocation request is important. The Holder/Customer may be represented by an authorized/delegated person at the RA in the matter of certificate revocation. The person representing the Certificate Holder/Customer must present a certified power of attorney or authorization, the text of which clearly expresses the will of the Certificate Holder/Customer to revoke the Certificate.

The RA may refuse a request to revoke a certificate if the Holder/Customer fails to authenticate his/her identity. The RA must verify the validity of the certificate to be revoked. The RA shall, if necessary, assist the Revocation Requestor in identifying the serial number of the certificate in question so that the certificate to be revoked can be uniquely identified. In the case of 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 has already been revoked.


In the event of a legitimate request for revocation and successful verification of the identity of the Holder/Customer, the certificate must be revoked as soon as possible.

Time for certificate revocation

CA must:

- revoke the certificate no later than 24 hours after verifying that the request for revocation of the certificate in question is justified,
- publish the current CRL and any previous CRLs of revoked certificates so that they are accessible to Customers/ Holders and all relying parties,
- inform the Customer/Certificate Holder of the revocation of their certificate by sending an email to the email address provided by the Holder during the RA

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	38 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

registration process, including the reason for the revocation of the certificate in question,

- archive all CRLs issued by him/her,
- synchronize the system time used as the source for the indication of the time of revocation of the certificate with UTC time at least every 24 hours.
- the CRL shall be published to the storage as soon as possible after it has been issued.

4.4.2 Suspension of the certificate

The provider does not support temporary suspension (suspension) of the certificate.

4.4.3 Certificate revocation list

Frequency of issuing CRL

Information about the revoked QC must be available on the Provider's website, which serves as its repository. The CP and CPS, or revisions thereto, must be published as soon as possible after their approval and issuance. All other information to be published in the repository must be published as soon as practicable.

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

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

CRL verification requirements

If information about revoked certificates is temporarily unavailable, then the party relying on the certificates must either refuse to use the certificate or make an informed decision accepting the risk, liability and consequences of using a certificate whose authenticity cannot be guaranteed according to the standards of this document. Such use of a certificate may occasionally be necessary to meet urgent operational requirements.

Between the time a legitimate request for revocation is made and the posting of the revoked certificate on the CRL, the Certificate Holder shall bear all responsibility for any damages caused by the misuse of its certificate. Once the certificate is published on the CRL, the party that relied on the revoked certificate shall bear all liability for any damage caused using the revoked certificate.


4.4.4 Verification of current certificate status

Verification of the status of the certificate is done through the current CRL published by the Provider.

Verification of the status of the certificate can be done manually via:

- Lists of current CRLs, as well as an archive of all issued CRLs for individual CAs of the Provider, available at:
<https://ocsp.nfqes.com/crl/>

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	39 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

- The Provider must ensure that a response is provided to a telephone or email enquiry sent or received via the Provider's helpdesk regarding the status of a particular certificate
- By means of a request to the appropriate OCSP responder, whose URIs of the OCSP responders of the Provider's individual issuing CAs are contained in the certificate extension (the request sent is in accordance with the requirements of RFC 6960)

4.4.5 Other applicable means of notification of certificate revocation

The RA responds to a query regarding the status of a specific certificate if the query was made by phone or email or by using the Provider's helpdesk, if the external RA has access to the helpdesk (if the external RA does not have access to the helpdesk, it responds only to phone and email queries).

4.5 Security audit

4.5.1 Types of events to be recorded

All events on the RA are recorded, as well as the interactions of Certificate Applicants and Certificate Holders with the RA. Records may be either electronic or written.

The records shall be viewable by the individual CMA components to the extent relevant to the activities they perform, the PMA, and by persons conducting compliance audits. Records shall be retained for a period, see Chapter 4.6.

Each RA unit must keep records of the activities of that RA unit by means of written or electronic records.

The records created represent the receipt of a certificate revocation request and the surrender of the certificate. In addition to these, all other events at the RA are recorded - mainly events related to the verification of the identity of the applicant, the RA private key (its compromise, receipt or loss of the smart card, forgetting the password), RA site security, receipt (and the manner of handling) of a complaint, comment or request for interpretation of the CP and CPS, rejected certificate requests, incoming requests, complaints, etc., and their handling, requests for sending the CRL and the Provider's certificate. The performance of inspections or audits on a given RA shall also be recorded.


The RA may make any entry concerning the Provider that it deems necessary or useful. The RA shall maintain all email correspondence regarding the Provider with other constituents and the external environment (customers, prospective customers, etc.). The RA department shall also keep all its written correspondence relating to the Provider.

4.6 Archival records

Archiving of records shall be carried out at regular intervals to ensure the long-term preservation of records in accordance with security requirements. Viewing of archived records shall be made available in its entirety to the PMA and compliance auditors. Modification or removal of archived information is not permitted.

The Provider shall keep all records of issued QCs as well as the QCs themselves in accordance with the requirements of the currently applicable legislation of the Slovak Republic. The

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	40 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Provider must keep the originals (or at least copies) of the application for the issue of certificates together with the relevant documents confirming the identity of the Holder in paper or electronic form for at least 10 years.

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, photocopy of identification documents, etc.).

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

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

4.7 Changing the key

The entire key change process must be carried out without negatively affecting the security level.

Provider key changes 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's key pair currently in use, a notice of the upcoming change of the Provider's 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 - the Provider must immediately notify the Supervisory Authority (NBÚ) (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 Provider's compromised key. The Provider must notify, via its website or by email or telephone, all Holders of QCs that have been signed with the Provider's revoked certificate, as well as Relying Parties, that the revoked Provider's certificate is to be removed from each application used by Relying Parties and replaced with a new Provider's certificate.

4.8 Contingency plan for emergencies

In case of compromise of the key of the root CA of the Provider or subordinate CAs, they are cancelled. Information about their cancellation must be published immediately in the fastest possible way.

The Provider shall notify all Holders of Certificates that have been signed with a revoked Provider Certificate, as well as the parties relying on those Certificates, that the revoked Provider Certificate is to be removed from any application used by the parties relying on the

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	41 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Certificates and is to be replaced by a new Provider Certificate. This must be distributed in a reliable manner.

In the event of a crash in which the Provider's equipment is damaged and inoperable, but its signature key is not destroyed, the CA must be restored to functionality as quickly as possible, prioritizing the ability to revoke certificates and publish up-to-date CRLs. In the event of a crash in which the CA installation is physically damaged and its signing key is destroyed as a result, the Provider's certificate shall be revoked. The CA installation is then completely repeated with the CA equipment restored, new Provider keys generated, a new CA certificate created, and new RA certificates created. Finally, all user certificates are re-issued using the new Provider certificate. The cost of creating new certificates to the entities affected by the creation of the new certificate shall be borne by the Provider in this case.

Parties relying on certificates may decide at their own risk to continue to use certificates signed using the destroyed private key to meet their urgent operational requirements. In the event of loss or damage to the smart card on which the External RA's certificate is stored, or in the event that the password to access the private key stored on that smart card is forgotten, or in the event that the smart card reader is inoperable, the External RA shall restrict or suspend its operations to the extent necessary and immediately notify the PMA of the event. In the case of a remote RA certificate, the same obligations as mentioned in the text above shall apply.

The functioning of the external RA shall be restored by revoking the RA certificate and creating a new RA certificate. This shall be promptly communicated to all components of the Provider and a new RA certificate shall be delivered to them in an appropriate manner.

A detailed description of the physical security measures is published in the Provider's current CPs, namely the CP NFQES CA and the CP NFQES ACA.

4.9 Termination of CA or RA

In case of termination of the Provider's or RA's activities for reasons other than events caused by force majeure (e.g. natural disaster, state of war, governmental decision, etc.), the procedure shall be in accordance with the provisions in Section 4.8.


The Provider shall make termination information available in an appropriate manner to Holders of all valid Certificates issued by it and to parties relying on the Certificates.

Appropriate means sending the information by:

- bulk e-mail via the Provider's IS,
- notifications of Certificate Holders in the Provider's IS,
- telephone conversation with Certificate Holders,
- distribution of this information via the Provider's website.

Upon termination of its activity, the Provider shall not issue any certificate and shall ensure demonstrable destruction of the signature data (private key). If the reason for the Provider's termination is for any reason unrelated to security, then neither the certificate of the terminating CA nor the certificates signed by the terminating CA need be revoked.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------


 NFQES BRAIN:IT	Version:	1.0
	Page:	42 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

Prior to termination, the RA shall provide archived data to the Provider component as directed by the PMA.

Prior to the termination of the provision of qualified services, the Provider must:

- give at least 6 months' notice of the planned termination of its activities to the Supervisory Authority (NBÚ), the Holders of all valid QCs issued by it, the parties relying on the QCs and the public, in an appropriate manner (see appropriate manner defined above), at least 6 months in advance,
- terminate any mandate agreements, powers of attorney, etc., under which others may have acted on behalf of the Provider (e.g., to provide RA services),
- terminate any QCs in force prior to termination if it fails to ensure continuity in the provision of its services,
- attempt to contract with another qualified trust service provider to ensure continuity in the provision of its qualified trust services,
- consolidate and archive all the Provider's documents,
- to carry out a control of compliance with the regulations on the protection of personal data, 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,
- remove from use all private keys, including copies thereof, in such a way that they cannot be recovered in any way.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	43 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

5 Physical, procedural and personnel security measures

The security of the Provider as well as the external RA 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 management. The security measures must be available to all personnel concerned.

The provider and the external RA must:

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

The security policy of the Provider and external RA and the overview of security-related assets must be reviewed regularly.

The Provider's and External RA's security policy and security asset overview must be reviewed in the event of significant changes to ensure their continuity, appropriateness, sufficiency and effectiveness.

Any changes that may affect the level of security provided must be approved by management.

The provider's and external RA's systems setup must be regularly reviewed for changes that compromise the security policy.

5.1 Physical security measures

Security mechanisms appropriate to the threat level in the external RA equipment environment shall be used to protect the external RA equipment.

A detailed description of the physical security measures is provided in the currently applicable CP NFQES CA or CP NFQES ACA, as appropriate.


5.2 Procedural security measures

Persons selected to hold RA roles must be responsible and trustworthy. The functions performed by this role are among the functions that form, on a personal level, the basis of trust in the entire NFQES CA and NFQES ACA.

Each RA operating under this document is subject to its provisions. The RA's primary responsibility is to:

- verification of identity through personal contact or through a proxy,
- recording information from Certificate Applicants and verifying its accuracy,
- secure communication with the Provider,
- distributing SSL Certificates received from the Provider,
- communicating with Certificate Applicants and Certificate Holders and documenting such communications.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	44 z 48
<i>OID „1.3.158.52577465.0.0.0.1.9.1“</i>	Document type:	Public

The person administering the component takes the role of Certificate Applicant and Certificate Holder in the case of hardware or software components (i.e., non-living systems) for which a certificate is issued. The person managing the component shall act in coordination with the CMA in registering components (routers, firewalls, etc.) in accordance with Section 3.1.9 and shall be responsible for fulfilling the obligations of Certificate Holders as defined in this document.


A detailed description of the procedural safeguards is published in the currently applicable CP NFQES CA or CP NFQES ACA, as applicable.

5.3 Personnel security measures

Personnel security measures are ensured by the internal mechanisms of the entity - the founder. Personnel for any role must be selected based on reliability, loyalty and trustworthiness. All persons holding RA roles of responsibility shall be properly briefed and trained. Topics to be covered include the operation of software and hardware used by the external RA as well as the CA, operational and safety procedures, the provisions of this document as well as the CP NFQES CA or CP NFQES ACA, as applicable.

Detailed descriptions of personnel security measures are published in the current CP NFQES CA or CP NFQES ACA, as applicable.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	45 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

6 Technical security measures

6.1 Key pair generation and installation

6.1.1 Key pair generation

This policy does not exclude any source of keys that have been generated in accordance with the provisions of this policy and local security requirements. It is assumed that the private key will be generated by the entity that becomes the owner of the key: e.g., the certificate applicant or RA, and on a device (e.g., computer, smart card or other token, HSM module, etc.) that is under the immediate control of the entity that becomes the owner of the generated key during key generation, or on the Provider's devices (remote certificate).

The private key shall not be allowed to get out of the security (HSM) module in which it was generated, unless it is encrypted for its local transmission or processing or storage.

An important security aspect that significantly limits the possibility of misuse of the private key belonging to the external RA is that the key pair of the external RA will be generated and stored on the smart card or in the Provider's devices (remote certificate). The process of generating the key pair on the smart card is initiated by connecting to the Provider's website with a suitable browser, opening the page through which the request for the personal certificate is generated (<https://zone.nfqes.com>) and selecting the appropriate key type. In the case of a remote certificate, the RA generates a CSR and sends it to the Provider for signature, which signs the received CSR with the private key and generates a certificate for the RA. Key generation is performed in a secure cryptographic key storage device that meets the legislative requirements for this type of device (HSM).

6.1.2 Delivery of the private key to the certificate Holder

No provisions.

6.1.3 Key length

The algorithms and key pair lengths applied in certificates have defined minimum key lengths for all entity types and all algorithms used.

Algorithms and key lengths applied in NFQES CA certificates:

Signature algorithm: *sha256RSA*

Public key: RSA 3072 bits or RSA 4096 bits

Algorithms and key lengths applied in the NFQES root CA certificate:

Signature algorithm: *sha256RSA*


Public key: RSA 4096 bits

Algorithms and key lengths applied in the certificate of child NFQES CAs:

Signature algorithm: *sha256RSA*

Public key: RSA 4096 bits

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	46 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

6.2 Private key protection

The certificate Holder must ensure that his private key never gets in unencrypted form outside the security module where it is stored. The basic principle is that no one should have access to the private key except the Certificate Holder. The Provider uses hardware cryptographic modules to protect the private keys of its issuing CAs.

Key Holders are allowed to back up their own key pairs. Keys must be encrypted during backup and transmission. The key holder is responsible for guaranteeing that all copies of private keys are protected, including the protection of all workstations on which any of its private keys reside. In the case of remote certificates and key pairs, the Holder cannot back up its key pairs.

Pass-phrases, PINs, biometrics, or other mechanisms of equivalent authentication robustness must be used to protect access to use the private key. Cryptographic modules that have been activated must not be left unattended or otherwise open to unauthorized access. Hardware cryptographic modules shall be removed and stored when not in use.

If activation data is written, it should be secured at the level of protection of the data that the cryptographic module is used to protect and should not be stored with it. Activation data for private keys belonging to certificates confirming individual identity should never be shared by more than one person. Activation data for private keys belonging to certificates confirming the identity of an organization or its organizational unit should be known only to those persons authorized to use the private keys in the organization.

An RA private key stored on a smart card shall never get outside the smart card on which it was generated, nor can it even be backed up. In addition, access to the private key stored on the card is protected by a password (pass phrase).


As a detachable piece of RA equipment, the chip card must not be left unattended in the card reader but must be inactivated by removing it from the reader whenever it is not in use. The chip card must be stored as securely as possible by the person using it, preferably in a lockable device (safety cabinet, safe, etc.). The activation data belonging to the smart card (i.e. the password for access to the private key stored on the card) must under no circumstances be recorded and stored with the smart card to prevent misuse of the private key stored on the card in the event of loss or theft of the card.

In the case of remote certificates, the Provider's private keys that are used in the production of issued QCs for end-users may be stored in a readable form in the HSM module itself. All HSM modules of the Provider are operated in secure premises with regime access.

6.3 Key pair management

All certificates issued by the Provider shall be archived for a further 10 years after their expiry or termination of the Provider's activity.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	47 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

7 Certificate profiles and list of revoked certificates

Certificate profiles and CRLs are set centrally - neither the customer nor any external RA can change the certificate structure.

7.1 Certificate profiles


The profiles of issued certificates are specified in the currently valid CP NFQES CA or CP NFQES ACA, as applicable.

7.2 Certificate Revocation list profiles

The profiles of revoked certificates are listed in the currently effective CP NFQES CA or CP NFQES ACA, as applicable.

CRLs issued by the Provider shall be version 2 CRLs. CRLs issued shall be in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------

 NFQES BRAIN:IT	Version:	1.0
	Page:	48 z 48
OID „1.3.158.52577465.0.0.0.1.9.1“	Document type:	Public

8 Administration of specifications

8.1 Specification change procedures

The Provider's PMA may review and, if necessary, revise this document.

Errors, requests for updates, or proposed changes to this document are to be communicated to the RA. Such communication shall include a description of the change, the rationale for the change, and contact information for the person who made the change. All changes motivated by the PMA must be brought to the attention of the affected entities (see Section 8.2 of this document) within one month.

After the time allowed for consideration of the change proposal has elapsed, the PMA must accept, accept with modification, or reject the proposed change.

8.2 Publication and notification policy

The PMA shall publish publicly the information contained in this document. If a new version of the RA Rules (including external RA) is approved, it shall be published no later than prior to the Effective Date via the Repository (see Section 2.6 of this document) so that it is available to all Relying Parties at the time of the Effective Date. The approved version of the RA Rules shall be sent electronically to all External RAs sufficiently in advance of the effective date to allow them to prepare for implementation or published on the Provider's website. The NFQES CA is responsible for sending information about changes to this document.

8.3 Publication procedures

This document will be made fully available to the PMA, the Provider, the External RA, and the auditor conducting the audit of the Provider or External RA. The document will be made available to the public via the Provider's website and other appropriate means as necessary.

8.4 Concessions

The PMA has the right to decide whether a variation in the CMA's practice is acceptable under this document or whether the CA should propose a variation to this document. The PMA may grant relief from any requirement of this document to accommodate urgent, unforeseen operational requirements. When relief is granted, it is to be made public via the Provider's website so that Certificate Relying Parties are aware of the relief and either a change to this document is to be initiated or a specific time limit is to be set for the validity of the relief. Each relief must be recorded.

brainit.sk , s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
-----------------------	-----------------------------------	---------------