



NFQES

Number: PO-03	POLICY		
Name: Certification Policy NFQES TSA Time Stamp			
Previous no.:	Release Date: 1.5.2021 Effective Date: 1.5.2021	Date of current revision: 1.5.2023 Effective Date of Revision: 1.5.2023	Registr. sign and time limit:

	First and Last Name: Department/function	Signature Approver:	of	Date:
Created by:	Ing. Martin Berzák Security Manager			1.5.2023
Approved:	Ing. Eduard Baraniak CEO			1.5.2023

NFQES TSA Time Stamp Policy

Version: **1.1**

Effective date: 1.5.2023

NFQES, s. r. o.	The Great Diel 3323, Žilina 010 08	ID: 52577465
-----------------	---------------------------------------	--------------




 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	2 z 48

Table of Contents


1.	INTRODUCTION	5
1.1	Overview	5
1.2	Title and identification of the document	5
1.3	PKI participants.....	6
1.3.1	Certification authorities	6
1.3.2	Registration authorities.....	6
1.3.3	Users of	6
1.3.4	Relying parties	6
1.3.5	Other participants.....	7
1.4	Use of the certificate.....	7
1.4.1	Appropriate use of the certificate.....	7
1.4.2	Prohibited use of the certificate	7
1.5	Policy administration	7
1.5.1	Information about the provider and contact details	7
1.5.2	Contact person.....	8
1.5.3	The person who determines the suitability of the CPS for the certification policy.....	8
1.5.4	CPS approval procedures	8
1.6	Definitions and abbreviations	8
2.	DISCLOSURE AND RESPONSIBILITY FOR DATA STORAGE.....	11
2.1	Storage.....	11
2.2	Disclosure of certification authority information.....	11
2.3	Time or frequency of publication	11
2.4	Access controls to repositories.....	11
3.	IDENTIFICATION AND AUTHENTICATION.....	12
4.	OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATE.....	13
4.1	Application for a certificate.....	13
4.2	Requests for the issuance of a certificate for the authentication of a website	14
4.3	Issuance of the certificate	15
4.4	Receipt of the certificate.....	15
4.5	Using public keys and certificates.....	15
4.6	Renewal of certificate	16
4.7	Issuance of a subsequent certificate	17
4.8	Modifying the certificate.....	17

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	3 z 48

4.9	Certificate revocation	17
4.10	Services related to certificate status	20
4.11	End of service provision	21
5.	PHYSICAL, PERSONNEL AND OPERATIONAL SECURITY MEASURES.....	22
5.1	Physical security	22
5.2	Procedural precautions.....	23
5.3	Personnel security measures	24
5.4	Procedures for obtaining audit records	25
5.5	Archive of records.....	26
5.6	Change the key	26
5.7	Recovering from compromise and disaster	27
5.8	Termination of CA or RA	27
6.	TECHNICAL SAFETY MEASURES.....	29
6.1	Generating and installing a key pair	29
6.2	Private key protection and cryptographic module design	30
6.3	Other aspects of key pair management.....	31
6.4	Activation data	32
6.5	Computer security checks.....	32
6.6	Life cycle measures.....	32
6.7	Network security controls.....	33
6.8	Time stamp.....	33
6.9	Making and verification of the time-stamp	33
6.10	Time synchronization with UTC.....	34
7.	CERTIFICATE, CRL AND OCSP PROCESSES	35
7.1	Certificate Profile.....	35
7.2	Profile of CRL.....	37
7.3	Profile of OCSP.....	38
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	39
8.1	Frequency or circumstances of assessment.....	39
8.2	Identity/qualifications of the assessor.....	39
8.3	Relationship of the evaluator to the evaluated entity.....	39
8.4	Topics covered by the evaluation.....	39
8.5	Measures taken as a result of the shortfall.....	39
8.6	Announcement of results.....	39

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	4 z 48

9.	OTHER BUSINESS AND LEGAL MATTERS	40
9.1	Fees	40
9.2	Financial responsibility.....	40
9.3	Confidentiality of business information.....	41
9.4	Privacy Policy	42
9.5	Intellectual property rights.	43
9.6	Declarations and warranties	43
9.7	Disclaimer of warranties	44
9.8	Limitations of liability.....	44
9.9	Compensation	44
9.10	Duration and termination	45
9.11	Individual notifications and communication with participants.....	45
9.12	Amendments	45
9.13	Dispute resolution provisions.....	46
9.14	Applicable law	46
9.15	Compliance with applicable legislation.....	46
9.16	Miscellaneous provisions	47
10.	Links	48

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	5 z 48

1. INTRODUCTION

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

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

The requirements of this CP are aimed at the performance of a qualified trust service for the production of qualified electronic time stamps, (hereafter referred to as a „time-stamp“) used to support qualified electronic signatures or any application requiring proof that information existed prior to a given time. The requirements of this policy are based on the use of public key cryptography, public key certificates and a reliable time source.

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

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

1.1 Overview

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

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

- **Qualified trusted service for issuing qualified electronic time-stamps**

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

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


1.2 Title and identification of the document

Document version: 1.1

Effective date: 1.5.2023

The NFQES TSA timestamp policy is identified by the OID object identifier 1.3.158.52577465.0.0.0.1.5.1, where the individual components of the OID have the following meanings:

- 1 ISO

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	6 z 48

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

History of change:

Version	Date	Description of the revision
1.0	1.5.2021	First approved version of the document
1.1	1.5.2023	Revision of the document

1.3 PKI participants

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

1.3.1 Certification authorities

Certification Authority:

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

The Provider's certification authorities are:

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

1.3.2 Registration authorities

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

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


1.3.3 Users of

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

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

1.3.4 Relying parties

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	7 z 48

1.3.5 Other participants

Policy Management Authority

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

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

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

1.4 Use of the certificate

A QC made for time-stamps where the private key is located on the QSCD is made for the purpose of supporting the Qualified Trust Service for the creation of qualified electronic time-stamps within the meaning of Article 3 (34) of the eIDAS Regulation.

1.4.1 Appropriate use of the certificate

No provisions

1.4.2 Prohibited use of the certificate

No provisions

1.5 Policy administration

1.5.1 Information about the provider and contact details

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

Headquarters: Veľký Diel 3323, 010 08 Žilina

ID: 52577465

IČO: 2121068763

IČ DPH: SK2121068763


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

Contact:

Mobile: +421 918 022 030

E-mail: info@brainit.sk

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	8 z 48

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

Supervisory authority:

Contact for Certificate cancellation request:

Mobile: +421 918 022 030

E-mail: info@nfqes.sk

1.5.2 Contact person

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

Certification Authority CA NFQES:

Address Veľký Diel 3323, 010 08 Žilina

Email: ca@nfqes.sk

Phone: +421 905 320 821

Website: <https://nfqes.sk>

To report incidents: infra@nfqes.sk

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

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

1.5.4 CPS approval procedures

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

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


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

1.6 Definitions and abbreviations

Certificate:

- a certificate or a qualified certificate for electronic signature within the meaning of the eIDAS Regulation;
- a certificate or a qualified certificate for an electronic seal within the meaning of the eIDAS Regulation;
- certificate for authentication of the website in accordance with the eIDAS Regulation;
- any other certificate used for encryption, authentication or other purposes as defined in the Provider's Policy, which has been or is to be issued by the Provider to the Customer.

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	9 z 48

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

These are mainly:

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

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

Regulation eIDAS - Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

OCRA token - a hardware token that conforms to the RFC 6287 standard - OCRA: OATH Challenge-Response Algorithm.

Provider Policy / Provider Policies -

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

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

Provider - the company brainit.sk, s. r. o. with the registered office at Veľký diel 3323, Žilina 010 08, IČO: 52577465, registered in the Commercial Register of the District Court of Žilina, Section Sro, Insert No. 72902/L.


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

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

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

General Terms and Conditions or abbreviated as GTC - this document General Terms and Conditions for the provision and use of the trusted service of issuing and verifying certificates, always in their effective version.


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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	10 z 48

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

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

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	11 z 48

2. DISCLOSURE AND RESPONSIBILITY FOR DATA STORAGE

2.1 Storage

The storage sites must be located to be accessible to Customers and Relying Parties and in accordance with overall security requirements.

The website will serve as the Provider's storage. The exact URL is set out in Chapter 1. The Provider's website is publicly accessible via the Internet to Customers, Relying Parties and the public.

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

2.2 Disclosure of certification authority information

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

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

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

2.3 Time or frequency of publication


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

CPs and CPSs, or revisions thereto, must be published as soon as possible after their approval and issue.

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

2.4 Access controls to repositories


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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	12 z 48

3. IDENTIFICATION AND AUTHENTICATION

The provisions of Chapter 3 of the NFQES CA Certification Policy apply

(OID: 1.3.158.52577465.0.0.0.1.3.2)

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	13 z 48

4. OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATE

4.1 Application for a certificate

4.1.1 Who can apply for a certificate

The provider may request the issue of:

- KC made for time-stamps
 - any entity (the Customer) which, under applicable national legislation, has the authority to act on behalf of the legal entity in question.

4.1.2 Registration process and responsibilities

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

- to familiarize themselves with the GTC for the provision and use of the trusted service of issuing and verifying certificates brainit.sk, s.r.o. and the information on the processing of personal data, which must be available in a readable form through a permanent communication channel (see zone.nfqes.sk),
- familiarize yourself with the procedure and, where appropriate, the principles and guidelines for obtaining QC,
- prepare the values of the individual items of the QC request so that these values are consistent with this CP,
- prepare your chosen identity documents or other necessary documents,
- in case of registration using RA to arrange a date for a visit.

Procedure before issuing the QC

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

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


4.1.3 Generating a request

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

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

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

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	14 z 48

4.1.4 Sending a certificate application

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

4.2 Requests for the issuance of a certificate for the authentication of a website

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

4.2.1 Performing identification and authentication functions

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

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

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

4.2.2 Approval or rejection of certificate applications

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


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

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

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

If the QC cannot be issued for a given request for any reason, the RA must inform the Customer of this fact.

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	15 z 48

4.2.3 Time for processing certificate applications

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

4.3 Issuance of the certificate

4.3.1 CA actions during certificate issuance

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

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

The issuance of a QC on a key pair generated directly at the RA shall be securely bound to the procedure of that generation.

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

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

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

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

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

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

4.4 Receipt of the certificate

4.4.1 Behaviour that constitutes acceptance of a certificate

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

4.4.2 Publication of the certificate.


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

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

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

4.5 Using public keys and certificates

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	16 z 48

4.5.1 Using a subscriber's private key and certificate

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

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

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


4.5.2 Use of a public key and relying party certificate

The relying parties are obliged to:

- use the QC only for the purpose for which it was issued,
- verify each QC for validity (i.e., verify that the QC is valid at the time and is not on the Provider's current list of cancelled QCs) before relying on the QC,
- establish a trust relationship with the CA that issued the QC by verifying the certification path in accordance with the X.509 version 3 standard and the mandatory use of the trusted list of the country in which the issuer resides, as specified in the countryName entry of the issuer's name in the 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.

4.6 Renewal of certificate

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	17 z 48

4.7 Issuance of a subsequent certificate

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

4.7.1 Conditions for the issue of a subsequent certificate

No provisions.

4.7.2 Who can apply for a subsequent certificate

A subsequent QC may be applied for by an existing Holder to whom it has been previously issued by the Provider and who meets the identification and authentication requirements of paragraph 3.2.

4.7.3 Processing requests for the issuance of a subsequent certificate

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

4.7.4 Notification of the issue of a subsequent certificate

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

4.7.5 Behaviour that constitutes acceptance of a subsequent certificate

See paragraph 4.4.

4.7.6 Publication of the subsequent certificate

See paragraph 4.4.2.

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

No provisions

4.8 Modifying the certificate


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

4.9 Certificate revocation

4.9.1 Conditions for certificate revocation

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

- the QC Holder shall request revocation of the certificate,
- finds that the requirements of the eIDAS Regulation or Act No. 272/2016 Coll. have not been met when issuing the QC,
- the court shall order the Provider to dissolve the QC by its decision,
- finds that the QC has been issued based on false information,

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	18 z 48

- learns that the QC Holder has died, if a natural person, or if a legal entity has ceased to exist,
- discovers that a private key belonging to the QC has been compromised, e.g. if access to a private key belonging to a public key listed in the QC is known to a person other than the Holder listed in the QC,
- the Holder has breached its obligations under this CP and/or the GTC,
- it becomes aware that the information on the certificate has become outdated,
- becomes aware that the Holder has become incapacitated by a court order,
- the Provider's private key has been compromised.

4.9.2 Who can apply for certificate revocation

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

He/she may also request the revocation of his certificate:

- the provider - the employee in question is obliged to document this fact, including the reason for his/her action,
- an entity (natural person or legal entity) based on the inheritance procedure (the Provider must attach to the documents on the dissolution of the QC a copy of the documents from which the right of the entity to apply for the dissolution of the QC is derived),
- the court through its judgment or interim measure (the Provider must attach a copy of the relevant court decision to the documents on the cancellation of the QC),
- a person authorized by the court, e.g. the guardian of the QC entity to be dissolved (the Provider must attach a copy of the relevant court decision to the documents on the dissolution of the QC).

4.9.3 Procedure for requesting the revocation of a certificate


Revocation of the QC must be requested by the authorized person in person at the Provider. The person requesting revocation of the QC must undergo the same authentication process with the Provider as required for the initial registration of the Holder/Customer (see paragraph 3.2), or provide the agreed password for cancellation of the QC, which will be provided to the Holder/Customer upon issuance of the QC.

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

The Holder/Customer of the QC may be represented by an authorized person with the Provider in relation to the cancellation of the QC. The representing person must present a certified power of attorney or authorization, the text of which clearly expresses the will of the Holder/Customer to cancel the QC.

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

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	19 z 48

If a legitimate request for revocation of a QC and successful verification of the identity of the Holder/Customer, the QC must be revoked as soon as possible (see clause 4.9.5).

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

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

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

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

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

4.9.5 Time within which the CA must process the revocation request

The provider must:

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


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

4.9.6 Cancellation control requirement for relying parties

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

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

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	20 z 48

4.9.7 Frequency of issuing CRLs

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

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

4.9.8 Maximum latency for CRL

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

4.9.9 Availability of OCSP service

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

4.9.10 OCSP inspection requirements

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

4.9.11 Other forms of availability of certificate revocation information

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

- Lists of current CRLs as well as an archive of all issued CRLs for individual certification authorities of the Provider, which are available at:
 - <https://zone.nfqes.sk/crl/>
- The Provider must ensure that a telephone or email enquiry regarding the status of a particular certificate is answered.

4.9.12 Special requirements for changing keys after they have been compromised

No provisions.

4.9.13 Circumstances in which the QC is suspended


Pursuant to Section 7 (2) of the Act on Trust Services 272/2016 Coll., a qualified trust service provider to which the qualified status has been granted by the Authority may not temporarily suspend a QC for electronic signature or a QC for electronic seal.

4.9.14 Who can apply for suspension of QC

No provisions.

4.10 Services related to certificate status

4.10.1 Operational requirements

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	21 z 48

The CRL shall be available at the URL specified in clause 4.9.11 and shall be accessible via HTTP protocol on port 80.


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

4.10.2 Service availability

Service availability is 24/7 at SLA level 99%.

4.11 End of service provision

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	22 z 48

5. PHYSICAL, PERSONNEL AND OPERATIONAL SECURITY MEASURES

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

The safety precautions must be available to all workers concerned.

The provider must:

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

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

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

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

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

5.1 Physical security


5.1.1 Premises

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

5.1.2 Physical access

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

5.1.3 Power supply and air conditioning

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	23 z 48

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

5.1.4 Protection from water

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Backup off the main site

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

5.2 Procedural precautions

5.2.1 Trusted roles

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

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

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


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

5.2.2 Number of persons required for the task

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

5.2.3 Identification and authentication for each role

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	24 z 48

5.2.4 Roles requiring division of responsibilities

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

5.3 Personnel security measures

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

5.3.1 Qualification, experience, and vetting requirements

Staff in trusted roles must meet qualification and experience requirements and should have security clearances of a specified level.

Persons in managerial positions must:

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

5.3.2 Verification requirements

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

5.3.3 Requirements for training

For some trusted Provider roles, there may be specific training requirements that should be completed prior to or during the assignment. Topics should include the operation of CMA software and hardware, security and operational procedures, provisions of this CPS, CP, etc.

5.3.4 Training renewal frequency

For roles where there are requirements to complete prescribed training, the need to repeat the training after completion of the primary training can be established.


5.3.5 Roll rotation frequency

No provisions.

5.3.6 Penalties for unauthorized conduct

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

Any inappropriate or unauthorized conduct by an employee in a trusted role identified by the Provider's management shall result in immediate removal from the trusted role pending completion of the ongoing management review. After management review and mutual discussion or review of the results of the investigation with the employee, the employee may be discharged from employment or reassigned to a trusted role, as appropriate.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	25 z 48

5.3.7 Requirements for external suppliers

Independent contractors who might be assigned to perform trusted roles shall be subject to the same obligations and specific requirements for those roles under the provisions of clause 5.3 and shall be equally subject to the sanctions set out in clause 5.3.6.

5.3.8 Documentation provided by the employee

Employees in trusted roles must be provided with the documents necessary to perform the function to which they are assigned, including a copy of this CP or CPS and all technical and operational documents necessary to maintain the integrity of the Provider's operations. This information must also include security and internal system documentation, identity verification procedures and policies, as well as other information prepared by the Provider and third-party or Internet-accessible documents.

5.4 Procedures for obtaining audit records

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

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

5.4.1 Types of recorded events

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

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

5.4.2 Frequency of processing of audit records

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

5.4.3 Retention period of the audit report


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

5.4.4 Audit log protection

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

5.4.5 Audit log backup procedures

No provisions.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	26 z 48

5.4.6 Audit collection system (internal vs. external)

No provisions.

5.4.7 Notification of the entity initiating the audit

No provisions.

5.4.8 Vulnerability assessment

See point 5.4.2.

5.5 Archive of records

5.5.1 Types of archived records

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

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

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

5.5.2 Retention period for the archive

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

5.5.3 Archive protection

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

5.5.4 Archive backup procedures

No provisions.

5.5.5 Time stamp requirements for records

No provisions.

5.5.6 Archiving system


No provisions.

5.5.7 Procedures for obtaining and verifying archival information

No provisions.

5.6 Change the key

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	27 z 48

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

- The expiration time of the Provider's keys currently in use is approaching. This is the normal state - 14 days before the expiration of the Provider'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 situation - the Provider must immediately notify the Supervisory Authority and the public that the Provider's keys have been compromised. It must also immediately revoke the compromised certificate.

5.7 Recovering from compromise and disaster

5.7.1 Procedures for dealing with compromise and disasters

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

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

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

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

5.7.2 Computing resources, software or data are corrupted

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

5.7.3 Private key compromise procedures


In the event of a TSA private key compromise, the Provider must have procedures in place to restore a secure environment and procedures for distributing the public key to end users.

5.7.4 Maintaining business continuity after a disaster

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

5.8 Termination of CA or RA

In case of termination of the Provider's activities for reasons other than events caused by force majeure (e.g. natural disaster, state of war, decision of state power, etc.), the procedure shall be in accordance with clause 5.7.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	28 z 48


Before terminating the provision of services, the Provider must:

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

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

Upon termination of its activity, the Provider must ensure that the TSA signature data (private keys) cannot be demonstrably reused and must not issue any time-stamp.

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	29 z 48

6. TECHNICAL SAFETY MEASURES

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

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

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

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

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

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

6.1 Generating and installing a key pair

6.1.1 Generating key pairs

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

6.1.2 Delivery of the private key to the subscriber

Not applicable

6.1.3 Delivery of the public key to the certificate issuer

Not applicable


6.1.4 Delivery of the CA public key to relying parties

Not applicable

6.1.5 Key sizes

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

6.1.6 Public parameter generation and quality control

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	30 z 48

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

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

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

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

6.2 Private key protection and cryptographic module design

6.2.1 Cryptographic module standards and controls

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

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

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

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

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

6.2.3 Saving the private key

No provisions.

6.2.4 Private key backup

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


6.2.5 Private key archive

No provisions.

6.2.6 Private key transfer to or from the cryptographic module

See 6.2.4

6.2.7 Storing the private key on the cryptographic module

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	31 z 48

The Provider's private keys, which are used in the creation of time-stamps for end-users, can be stored in the HSM module itself in a readable form. All HSM modules of the Provider shall be operated in secure premises with regime access.

6.2.8 How to activate the private key

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

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

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

6.2.9 How to deactivate the private key

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

6.2.10 Method of destroying the private key

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

6.2.11 Cryptographic module evaluation

See point 6.2.1.

6.3 Other aspects of key pair management


6.3.1 Public Key Archive

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

6.3.2 Certificate operating periods and key pair usage periods

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

Type of certificate	Validity (maximum)
Issuing CA	30 years
KC for time stamps	10 years

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	32 z 48

6.4 Activation data

6.4.1 Generating and installing activation data

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

6.4.2 Activation of data protection

Key pair designed for TSA issuer:

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

6.4.3 Other aspects of activation data

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

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

6.5 Computer security checks

6.5.1 Specific technical requirements for computer security

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

A provider issuing QCs for TSA may follow the information security requirements for a trust service provider defined in ETSI EN 319 411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

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

6.5.2 Computer security assessment


No provisions.

6.6 Life cycle measures

6.6.1 System development checks

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

6.6.2 Safety management controls

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	33 z 48

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

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

6.6.3 Life cycle safety measures

No provisions.

6.7 Network security controls

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

6.8 Time stamp

NFQES TSA will ensure that the time-stamp is issued securely and that it contains the correct time, above all:


- a) the time-stamp contains the identifier of the timestamp policy,
- b) the time-stamp has a unique identification number,
- c) the value of the time to be put into the time-stamp to be produced will be derived from the real time value provided by UTC (as a reliable time source),
- d) the time that is fed into the time-stamp being produced is synchronized with the UTC value within the precision defined in this policy,
- e) if a TSA clock deviation is detected that exceeds the accuracy declared by this policy, TSA will not issue a NFQES time stamp,
- f) the time-stamp shall include the hash function value provided by the requester applied to the data for which the timestamp is to be produced,
- g) the time-stamp is signed with the TSA NFQES key, which is used for this purpose only

6.9 Making and verification of the time-stamp

The applicant shall send (via an agreed interface) to the TSA NFQES, as the time-stamp issuer, a request for a time-stamp. The request shall include a digital impression of the document to be time-stamped, created using an approved hashing function. If the request is in an approved format and there are no impediments to the NFQES TSA making the time-stamp, the NFQES TSA shall, using a secure time-stamping device and time source, make a time-stamp on the submitted digital impression of the document and send it online to the requester. If the time-stamp request is not in an approved format, or if the TSA NFQES has encountered obstacles to the time-stamp (e.g., a time deviation outside of the stated accuracy has been detected), the TSA NFQES shall not time-stamp the submitted digital document impression and shall inform the applicant online of this fact and the reason for it. Validation of the time-stamp shall be performed by the relying party based on the time-stamp and the document on which the time-stamp was made and the time stamp policy that applies to the time-stamp.

The time-stamp is valid if:


- the enhanced electronic time-stamp signature is valid,
- the time-stamp is consistent with the time-stamp policy used.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	34 z 48

6.10 Time synchronization with UTC

TSA NFQES shall ensure that the time used by it is synchronized to UTC with a declared accuracy of less than 1 second, primarily by the following measures:

- a) calibration of the TSA NFQES clock will be performed such that the expected time deviation will not be outside the declared accuracy,
- b) TSA NFQES device clocks will be protected against threats that could lead to undetectable clock tampering that could cause them to deviate from their calibration,
- c) TSA NFQES will ensure that if the time that would have been indicated on the time-stamp is out of sync with UTC, this will be detected and the time-stamp will not be issued,
- d) the NFQES TSA will ensure that a clock synchronization will be performed if notified by an authorized authority of the occurrence of a correction second.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	35 z 48

7. CERTIFICATE, CRL AND OCSP PROCESSES

7.1 Certificate Profile

The QC profiles, CRL profiles and the response in the form of certificate validity information provided via the OCSP protocol shall be centrally determined by the PMA and neither the persons holding the service levels (roles) may arbitrarily change the structure of these profiles or responses.

The structure of the QCs produced by the Provider may only be changed at the decision of the PMA's delegated member.

7.1.1 Version numbers


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

7.1.2 Certificate parameters

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

7.1.3 Certificate Extension

Name of the extension	ASN.1 Name and OID/Description	Presence	Criticality
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Specifies (http:// ... p7c, certificate or also ldap://...) the address to obtain certificates issued for the issuer of this certificate and the address to OCSP.	Yes	No
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} The Certificate Holder's public key identifier.	Yes	No
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} The public key identifier of the CA that issued this certificate.	Yes	No

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	36 z 48

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


7.1.4 Algorithm object identifiers

Signature Algorithm for QCs (Signature Algorithm)

sha256RSA OID: 1.2.840.113549.1.1.11

7.1.5 Forms of names

The Provider identifier in the form "TSA NFQES" must always appear on the issuing TSA certificate.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	37 z 48

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

Key lengths and KC validity: public key

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

7.1.6 Restrictions on names

No provisions.

7.1.7 Certification policy identifier

See chapter 1.2

7.1.8 Using extensions to restrict the policy

This extension is not used.

7.1.9 Syntax and semantics of politics

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

7.1.10 Extension

No provisions.

7.2 Profile of CRL

7.2.1 Version numbers

CRLs issued by the Provider must be CRL version 2.


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

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

7.2.2 CRL and CRL input extensions

Extensions to the CRL issued:

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	38 z 48

7.3 Profile of OCSP


7.3.1 Version numbers

If the Provider issues OCSP responses, these must be in accordance with RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". If OCSP responses will be issued by separate OCSP responders for each of the Provider's CAs issuing QCs, their signing certificates shall be signed by the corresponding Provider CAs and shall include an extension for the use of the OCSP Signing Key (1.3.6.1.5.5.7.3.9).

7.3.2 OCSP Extensions

Extensions in the OCSP response:

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	39 z 48

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of the assessor

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

8.3 Relationship of the evaluator to the evaluated entity

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

8.4 Topics covered by the evaluation

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

8.5 Measures taken as a result of the shortfall


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

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

8.6 Announcement of results

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

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	40 z 48

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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

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

9.1.1 Fees for the issue or renewal of a certificate

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

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

9.1.2 Fees for access to the certificate

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

9.1.3 Fees for appeal or access to status information

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

9.1.4 Charges for other services

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

9.1.5 Refund Policy

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

9.2 Financial responsibility

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


9.2.1 Insurance cover

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

9.2.2 Other assets

No provisions.

9.2.3 Insurance or guarantee for end-users

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	41 z 48

No provisions.

9.3 Confidentiality of business information

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

9.3.1 Scope of confidential information

Confidential information subject to appropriate protection is:

- internal infrastructure (e.g. documents, procedures, files, scripts, passwords, pass phrases, etc.) used for the operation of the Provider, including its RA, the Provider's private keys used for signing the executed QCs,
- OCSP responder private keys used to sign responses to requests to confirm the existence and validity of the QC,
- TSA private keys used to create qualified electronic time-stamps.

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

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

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


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

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

9.3.3 Responsibility for the protection of confidential information

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

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	42 z 48

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

- compulsory disclosure in criminal, civil or administrative proceedings,
- mandatory provision of information to the supervisory authority,
- the provision of information at the request of the data subject.

9.4 Privacy Policy

9.4.1 Data Protection Plan

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

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

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

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

- a) always available in electronic form on the Provider's website,
- b) sent in electronic form to the Customer's/Holder's email address prior to the commencement of the provision of trust services, and
- c) available in paper form from the Provider.

9.4.2 Information considered private

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

9.4.3 Information that is not considered private


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

9.4.4 Responsibility for the protection of private information

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

9.4.5 Notification and consent to the use of private information

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	43 z 48

9.5 Intellectual property rights.

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

9.6 Declarations and warranties

The Provider, through this CP, expresses the legal presumptions for the use of the issued qualified time-stamps.

9.6.1 CA representations and warranties

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

The Provider reserves the right, if it deems it appropriate, to change these declarations at its own discretion or in accordance with applicable legislation.

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

- comply with its obligations under this CP, the issued CPS as well as other published policies and procedures, including the Information Security Policy,
- fulfilment of its obligations under the eIDAS Regulation and the applicable legislation of the SR,
- immediately informing the subjects concerned in the event of compromise of their private keys in accordance with this CP,
- implementing security mechanisms, including mechanisms for private key generation and protection, relating to the protection of its PKI infrastructure,
- the availability of printed or electronic versions of this CP and other published policies online,
- compliance with the Data Protection Regulations when handling personal data of Customers.


9.6.2 RA Declaration and Warranties

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

9.6.3 Declarations and warranties of participants

Unless otherwise specified in this CP or the applicable Customer Agreement, the Customer is solely responsible for:

- providing accurate and correct information in communication with the Provider,
- read and agree to all the terms and conditions set out in this CP and its associated policies, which are available on the Provider's repository (see Chapter 1),
- use of issued QCs only for legal and authorization purposes in accordance with this CP,
- terminate the use of the QCs if any information in them proves to be misleading, outdated, or incorrect,

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	44 z 48

- use its best efforts to prevent compromise, loss, declassification, modification, or any unauthorized use of the private key corresponding to the public key contained in the QC issued by the Provider.

9.6.4 Representations and warranties of the relying parties

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

9.6.5 Representations and warranties of other participants

No provisions.

9.7 Disclaimer of warranties

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

9.8 Limitations of liability

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


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

- a) breach of the obligations of the Customer or the Relying Party set out in generally applicable law, the relevant Contract, the GTC or the Provider's policies, including the obligation to exercise reasonable care in the use of and reliance on the Certificates,
- b) failure of the Customer to provide the necessary cooperation,
- c) the technical characteristics, incompatibility, configuration, unsuitability or other defects of the software or hardware used by them,
- d) using or relying on a certificate that has expired or been revoked,
- e) non-delivery or delay of requests to verify the status of the certificate to the Provider, for reasons that are not on the Provider's side (in particular, cases of unavailability or congestion of the Internet network or defects in the equipment or technical equipment used by the verifier),
- f) failure to provide any of the trusted services or their unavailability during planned maintenance or reorganization announced on the Provider's website,
- g) the action of a higher power,

The Provider shall not be liable for any damages incurred by the Relying Party due to the Relying Party's failure to follow Chapter 10 of the GTC and this CP when relying on the Provider's trusted services. or the Relying Party information.

9.9 Compensation

Whoever breaches his/her duty or any obligation arising from this CP, the Contract and the GTC is obliged to compensate for the damage caused to the other party, except in cases where the liability of

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	45 z 48

the entity for damages is excluded. Damages shall be deemed to be actual loss, loss of profit and costs incurred by the injured party in connection with the damage event.

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

9.10 Duration and termination

9.10.1 Deadline

This version of the CP is valid from the date of its entry into force, i.e. 1.5.2021, until it is replaced by a new version. Details of the change history of this CP are set out at the beginning of the document in the 'History of change' section.

9.10.2 End

The validity of this version of the CP shall expire on the date of publication of a new version with a higher number than 1.0, or on the date of termination of the activity of provision of qualified trust services by the Provider at the time of its validity. All revisions to the CP and CPS that are listed in the change history for that document must be made available to Customers and Relying Parties, respectively.

9.10.3 Termination and survival effect

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

9.11 Individual notifications and communication with participants

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


9.12 Amendments

9.12.1 Amendment procedure

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

Approval of the proposed changes must be made by an authorized PMA member. Proposed changes must be considered within 14 days of receipt. After the expiry of the time limit for consideration of the proposed change, the PMA must accept, accept with modification, or reject the proposed change.

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	46 z 48

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

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

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

9.12.2 Mechanism and notification period

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

Internal staff shall be equally informed about the new version of this CP.

9.12.3 Circumstances in which the OID must be changed

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

9.13 Dispute resolution provisions

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

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

In this case, the Customer is entitled to contact an out-of-court dispute resolution entity, which is the Slovak Trade Inspection, or another legal entity registered in the list of alternative dispute resolution entities maintained by the Ministry of Economy of the SR and available on its website, the 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.


9.14 Applicable law

Legal relations between the Provider and the Customer are governed by the laws of the SR.

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


9.15 Compliance with applicable legislation

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

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	47 z 48

9.16 Miscellaneous provisions

No provisions.

 NFQES	Version:	1.1
OID: 1.3.158.52577465.0.0.0.1.5.1	Page:	48 z 48

10. Links

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Regulation (EU) No 910/2014 and Corrigendum
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
- Act No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amending and supplementing certain acts (hereinafter referred to as the Trust Services Act)
- Act No. 18/2018 Coll. on Personal Data Protection
- Information on the processing of personal data (version 1.0)
- General Terms and Conditions of Provision and Use of the Trusted Service for the Execution and Verification of Certificates brainit.sk, s.r.o. effective from 1.12.2020 (version 1.1)
- SD Supervisory scheme for qualified trust services as defined by the supervisor
- ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC6960)