NFQES ACA - AdES Certification Policy

Version: **1.1**

Effective date: 1.1.2024

PO-09

Policy

Public

Created by:
Ing. Martin Berzák
Security Manager

23.11.2023

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

23.11.2023

brainit.sk, s. r. o.

Veľký Diel 3323, 010 08 Žilina
ID: 52577465

www.brainit.sk

History of changes

Version	Date	Authors	Description	Reason for changes
1.0	1.3.2023	Ing. Martin Berzák	First approved version of the document	
1.1	23.21.2023	Ing. Michal Šterbák, PhD.	Modified and approved version of the document	

Table of Contents

1. INTRODUCTION

The NFQES ACA - AdES Certification Policy in the current version is the certification policy for advanced electronic signature/seal, of the NFQES Certification Authority (hereinafter referred to as "CP") is a document describing the general rules, regulations, binding procedures, methodology and responsibilities applied by the company brainit.sk s. r. o., 52577465, registered in the Commercial Register of the District Court of Žilina, Section Sro, Insert No. 72902/L (hereinafter referred to as "Provider" or "brainit.sk") in the creation and management of advanced certificates for advanced electronic signatures/seals, the types of certification services applicable to these certificates, as well as the scope of their use for a given certification authority (hereinafter referred to as "CA").

When issuing an advanced certificate (AdC) for an advanced electronic signature/seal from brainit.sk s. r. o., procedures are in place to ensure a high level of reliability and security of the authenticated information identifying the customers defined in more detail in point 1.3.3 (hereinafter referred to as "Customer"). Procedures are in place to ensure reliability and security in the issuance, disclosure and management (renewal, termination, invalidation) of enhanced certificates, signatures, private key storage and its use in applications.

This CP is an important document especially for customers (signatories) and relying parties (further defined in 1.3.4) in terms of the feasibility of these services.

The relationship between brainit.sk, s. r. o. and the customer are governed by a contract between them, which is concluded for improved certification services, or by remote acceptance when using the NFQES SaaS platform available at https://zone.nfqes.com. Prices for certificates and services for the issuance and management of enhanced certificates are set out in the price list available on the NFQES Client Zone website.

The CP is a binding document, serving as a standard of practices, procedures and principles to be followed by all parties involved in the provision of trust services by the Provider.

The Provider's website is at https://nfqes.com

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

1.1. Definitions and abbreviations

1.1.1. Definitions

Certification - a Certification Service Provider may be granted "enhanced" status for a specific period in accordance with Regulation (EU) No 910/2014 following a successful compliance audit by accredited auditors**.**

Certificate:

- advanced certificate for providing advanced electronic signature
- any other certificate used for encryption, authentication or other purposes within the meaning of this CP and the Provider's CPS that has been or is to be issued by the Provider to the Customer.

CRL – Certificate Revocation List - a list of revoked certificates before their expiry date.

Validation data - data that is used to verify the electronic signature/seal.

Validation - the process of verifying and confirming that an electronic signature or seal is valid.

Personal identification data - a set of data that makes it possible to establish the identity of a natural person or legal entity or a natural person representing a legal entity.

Electronic signature creation data - unique data used by the signer to create an electronic signature.

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...

Advanced electronic signature - is a signature that is created by an application/system for the creation of an advanced electronic signature and that is based on an advanced certificate for electronic signatures.

Advanced Electronic Seal - is a seal that is created by an Advanced Electronic Seal application/system and is based on an Advanced Electronic Seal Certificate.

Coordinated Universal Time (UTC) - the time to which time in different time zones is calculated. It uses International Atomic Time (TAI) as a basis.

The CPS - Certificate Policy Statement for the Practice of Providing Enhanced Certification Services is a document containing rules for the issuance, suspension, revocation and invalidation of certificates, as well as the conditions for granting access to certificates.

Private key - a string of symbols used in an algorithm to convert information from readable to encrypted form or vice versa.

Public key - one of the key pairs used in asymmetric cryptography that is accessible and can be used to verify an electronic signature/seal.

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

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

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

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

Provider Policy / Provider Policies -

- the policy of the trust service provider for issuing and verifying enhanced certificates, which applies to enhanced certificates issued by the Provider in accordance with the eIDAS Regulation,
- a policy for the provision of a trusted service for the production and verification of Enhanced Certificates, applicable to other Certificates not listed in the paragraph above.

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, ID No.: 52577465, registered in the Commercial Register of the District Court of Žilina, Section Sro, Insert No. 72902/L.

RA Operator - the entity that operates the registration authority of the Provider

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 entity who relies on the Provider's Trusted Services to act.

General Terms and Conditions or abbreviated as GTC - the document "General Terms and Conditions", always in their effective version available on the Provider's website.

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.

1.1.2. Abbreviations

AdC - Advanced Certificate

QCP-l - Qualified Certificate Policy issued to a legal entity when the private key of the associated certificate is generated in a secure environment.

QCP-n - Qualified Certification Policy issued to an individual when the private key of the associated certificate is generated in a secure environment.

NCP+ - Enhanced Standardised Certification Policy, which includes additional requirements for enhanced certificates in accordance with Regulation (EU) No 910/2014.

CN - Common Name

CPS - Certification Policy/Practice Statement

HSM - Hardware Security Module

LDAP - Lightweight Directory Access Protocol

PKI - Public Key Infrastructure

PO - legal entity

RA - Registration authority

SHA - hash algorithm for hash identifier extraction (Secure Hash Algorithm)

SSL - Secure Socket Layer (SSL)

SR – Slovak Republic

SMIME - Secure Multipurpose Internet Mail Extensions

IETF - Internet Engineering Task Force

RFC - Request for comments

1.2. Overview

The CP Document applies to enhanced certificates issued by the Provider pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/ES. The CP complies with the applicable legislation of the Slovak Republic (SR). The document is structured in accordance with the framework defined in 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 certificate management according to the X.509 standard in the implementation of the Public Key Infrastructure (hereinafter "PKI").

The issuance of Advanced Certificates (hereinafter referred to as "AdCs") for advanced electronic signatures/seals is associated with:

- **issuing an advanced certificate to a natural person (Signatory) - Advanced certificate for advanced electronic signature**
- **issuing an advanced certificate to a legal entity (Seal Creator) - Advanced Certificate for Advanced Electronic Seal**

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

Provider's Certification Authority	Certificate serial number	Publisher
ACA NFQES	4a2a267827944e5323683482e7d5a72205491ac1	CA NFQES

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

- ACA NFQES Certificate
- Certificate to validate the existence and validity of the certificate (OCSP)

1.3. Title and identification of the document

Document version: 1.1

Effective date: 1.1.2024

The CP document for an NFQES Advanced Electronic Signature/Seal is identified by an object identifier that relying parties can use to determine its applicability to an application as described in IETF Recommendation RFC 3647, Section 3.3. The CP is defined by OID 1.3.158. 52577465 .0.0.0.2.1.1, where the individual components of the OID have the following meanings:

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

The Provider ensures that it does not change the object identifier of this document, as well as the object identifiers of policies, procedures and other guidance documents. If there is an extension or update in the policy that does not affect previously issued certificates, the Provider shall update a new object identifier that covers the new certificates or the extended/updated certificates. The Provider shall follow its internal OID management procedure.

1.4. Infrastructure participants (PKI)

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

The Provider, as a provider of advanced certification services, provides services for the generation and management (suspension, renewal and termination) of advanced certificates through the authentication authority "NFQES ACA" and services for the identification and authentication of Customers through the Registration Authority (RA).

Other participants in the Provider's infrastructure are Customers and Relying Parties.

1.4.1. Certification authorities

Certification Authority:

- is an entity that provides advanced certificates for advanced electronic signatures/seals that are managed under this CP
- is part of the hierarchical PKI structure in the issued advanced certificates (AdC issuer)

The Provider's certification authorities are:

- The NFQES ACA (serial number: 4a2a267827944e5323683482e7d5a72205491ac1), which issues enhanced certificates to users and is part of the hierarchical PKI structure of the NFQES CA.

1.4.2. Registration authorities

The 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 for all Customers interested in advanced certificates for advanced electronic signatures/seals. This RA is not a separate legal entity.

RA carries out the following activities:

- receive applications for improved certificates, approve or reject these applications in accordance with internal approval rules
- verifies the identity of persons applying for certificates
- verifies that the issued certificate is handed over to the Customer
- terminates upgraded certificates based on expiration rules

1.4.3. Users, Customer, Participants

Any natural person or legal entity who has a written contract with the Provider is a customer of the advanced certification service provided by the Provider, while the Customer also pays for the services.

The holder of a AdC is the person named in the AdC. The Certificate Holder may be one person - the Customer, or two different persons, for example if the Customer is the employer but the Certificate Holder is an employee.

The holder of the AdC may be:

- the natural person (signatory) who creates the advanced electronic signature
- a natural person (signatory) who is an authorized representative of a legal entity and who executes an advanced electronic signature
- a natural person identified in connection with a legal entity
- a legal entity, which may be an organization or a unit or department thereof
- a legal entity that creates an advanced electronic seal

If the Customer is a natural person and only his/her name and surname are indicated as the subject, the Customer and the Holder of the AdC are the same natural person, i.e. in case of non-fulfilment of the obligations imposed on both the Customer and the Holder, this natural person is directly responsible.

When the Customer acts on behalf of one or more Holders with which it is connected (e.g. the Customer is a legal entity requesting the issuance of AdC for its employees), the different responsibilities of the Customer and the Holder are defined in the document "General Terms and Conditions" in the current version (hereinafter referred to as "GTC") published on the Provider's website:

https://nfqes.com/documents

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

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

When applying for a AdC of an individual (Holder), the Customer is

- the natural person himself,

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

- the statutory body of the legal entity applying on behalf of its subsidiaries or units or divisions.

1.4.4. Relying parties

Relying Parties are natural person or legal entity who accept the AdC issued by the Provider and rely on the Provider's trust service procedures in their actions.

1.4.5. Other participants

The Provider reserves the right, if necessary, to enter contracts with external parties for the provision of certain certification services.

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

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

Other service providers

Other service providers include:

- OCSP responder Provider that provides AdC validation services.

1.5. Use of the certificate

The AdC made for a natural person is made for the purpose of supporting an advanced electronic signature within the meaning of Article 3 point 11 of the eIDAS Regulation.

The AdC made for a legal entity is made for the purpose of supporting the improved electronic seal within the meaning of Article 3 point 26 of the eIDAS Regulation.

1.5.1. Appropriate use of the certificate

An AdC of a natural person, legal entity, or an authorized representative of a legal entity named in the certificate as a signatory can be used to create an advanced electronic signature/seal in electronic documents and attachments/transactions that require a high level of information security.

1.5.2. Prohibited use of the certificate

The Provider's enhanced certificates may not be used in a manner inconsistent with their stated purpose and scope/principles. Enhanced Certificates issued in accordance with this policy shall not be used for illegal purposes.

1.6. Policy administration

The provider is responsible for the management of this policy.

Each version of the Policy shall remain in force until a new version is approved and published. Each new version is developed by the Provider's staff and is published after approval by the Provider's CEO. Customers are only required to adhere to the version of the Policy in effect at the time they use the Provider's services.

1.6.1. Information about the Provider and its contact details

Name: brainit.sk, s. r. o.
Headquarters: Veľký Diel 3323, 010 08 Žilina
IČO: 52577465
DIČ: 2121068763
IČ DPH: SK2121068763
Register: the Commercial Register of the District Court of Žilina, section Sro, insert number 72902/L
Contact:
Mobile: +421 918 022 030
E-mail: info@brainit.sk
Provider's website: https://nfqes.com/
Trust Services website: https://zone.nfqes.com/
Contact for Certificate cancellation request:
Mobile: +421 918 022 030
E-mail: info@nfqes.sk

1.6.2. Contact person

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

NFQES ACA Certification Authority:

Address Veľký Diel 3323, 010 08 Žilina

Email: ca@nfqes.sk

Phone: +421 905 320 821

Website: https://nfqes.com

To report incidents: infra@nfqes.sk

1.6.3. The person who determines the suitability of the CPS for the certification policy

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

CP and CPS cover the same set of topics, serving users and relying parties, to provide a secure and reliable AdC application for advanced electronic signature/seal issued by the Provider.

The main difference between the two documents is the focus of their provisions and their intended purpose. The CP examines the requirements for the implementation of the necessary standards and infrastructure. In addition, the CP identifies the participants in certification services activities. The CPS, on the other hand, describes how CAs and other infrastructure participants apply procedures and controls to meet the requirements of the CP. In other words, the purpose of both documents is to provide uniform rules and procedures for how the Provider's infrastructure participants fulfill their duties and responsibilities.

1.6.4. 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 AdC.

Each version of the CP and CPS shall be valid until a new version approved and published on the Provider's website is effective. The publication of the approved new approved version is always, at least 30 days prior to its effectiveness , unless it is an extraordinary circumstance. An extraordinary circumstance is one that cannot be postponed.

2. DISCLOSURE AND RESPONSIBILITY FOR DATA STORAGE

2.1. Storage

The storage sites that holds current and prior versions of electronic documents must be located to be accessible to the AdC Holders and the Relying Parties and in accordance with overall security requirements.

The Provider manages and controls the Company's website, which acts as the Provider's storage. The exact URL address is given in Chapter 1. The Provider's website publishes all up-to-date versions of electronic documents and provides interested parties with secure and continuous access to these documents. The Provider's website is publicly accessible via the Internet to AdC Holders, Relying Parties and the public.

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

2.2. Disclosure of CA information

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

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

The CRL must be published as specified in Chapter 4.9.7. Information on the cancelled AdC must be available on the Provider's website (see Chapter 1), which serves as its repository.

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

All other information to be published on 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.

Provider offers access to the information stored on the repository, providing HTTP/HTTPS and OSCP-based access.

3. Identification, authentication and name verification

This chapter presents the general rules for user authentication applied by the Provider when issuing AdC. The rules are based on certain types of information that are included in the certificates. The exact procedures for checks and name entry are described in the CPS document of this CP.

3.1. Naming

The requirements for names/names for the certificate are defined in ITU-T Recommendation X.509 or IETF RFC 5280 and ETSI EN 319 412. Names may be consistent with the Domain Name System (DNS) service described in RFC 2247. The RA verifies and ensures that the names in the certificate request are compliant with the X.509 standard.

The "Subject" field on the certificate contains the name of the Signer (Author). The name and other distinguishing features of the Signer in the corresponding fields for each type of certificate are in accordance with the Distinguished Name (DN), which is formed according to the X.500 and X.520 standards.

The detailed specification of the certificates issued by the Provider is set out in other sections of this document as well as the CPS document of this CP.

3.1.1. Types of names

Each CA shall be able to generate certificates that contain X.500 Distinguished Names (X.500 Distinguished Name, hereafter referred to as "Distinguished Name"), specifically in accordance with X.501 and X.520 respectively, and names in accordance with RFC 5322 Internet Message Format.

Requirements for the names of issued certificates are specified in ITU-T Recommendation X.509 or IETF RFC 5280 and ETSI EN 319 412. The names may be in accordance with the Domain Name System (DNS) service described in RFC 2247. This method allows subscribers to use two types of names: DN and DNS.

3.1.2. The Need for meaningfulness of names

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

The names used must reliably identify the persons to whom they are assigned. In some cases, accented characters shall not be used in the content of the AdC and shall be replaced by equivalent ASCII character table characters (e.g., “á” shall be replaced by “a”; “č” shall be replaced by “c”, etc.). Such a case may be requested by the customer when the device on which the AdC is to be used is a dedicated HW that cannot be replaced (or is unprofitable for the customer) and does not support the UTF-8 character set.

3.1.3. Anonymity or pseudo-anonymity of subscribers

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

3.1.4. Rules for interpreting different forms of names

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

3.1.5. Uniqueness of names

The Provider is responsible for the clarity of names throughout the AdCs Holder community.

3.1.6. Recognition, authentication and the role of trademarks

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

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

The Provider shall not knowingly issue a AdC containing a name that has been determined by a court of competent jurisdiction to infringe the trademark of another entity. The Provider is not obligated to examine trademarks or resolve trademark disputes.

3.2. Initial identity verification

The initial registration of the Customer shall take place when the registration request is first sent to the Provider.

Registration includes procedures that allow for the collection of data about his identity as well as his identification before issuing a certificate. This data verification requires remote presence in front of an employee of the Provider or his/her RA, a notary public or other authorized person confirming his/her identity, or the data verification is mediated by an external RA. This procedure may be carried out remotely and, where possible, automated, using a remote identification system that meets the requirements of Regulation (EU) No 910/2014.

The Customer is obliged to submit/supply all the necessary information for unambiguous identification and verification of his/her identity:

- name and surname on the identity document
- proof of identity - ID card, international passport or other proof of identity
- national identification number, *date of birth if none*
- contact details - mobile phone, email and address

After successful verification of the Customer's identity, the authorized Operator in RA:

- offers GTC on advanced certification services signed on behalf of the Provider and keeps all documents attached to the contract
- acknowledge the certificate request and send the electronic certificate request
- records the issued certificate on a secure signature creation device and sends it to the Customer or authorized person

In case the Customer uses the remote identification option, he/she requests the remote service by submitting personal data as well as mobile number and e-mail. In this case, a contract between the Customer and the Provider is concluded and an advanced certificate for advanced electronic signature

is issued and the contract with the Provider is immediately signed. A registration profile is maintained for each person in the Provider's systems.

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

If an emergency is declared within the SR within the meaning of Act No. 42/1994 Coll. on Civil Protection of the Population, as amended, the PMA may decide to modify the method of issuing advanced certificates and the associated generation of cryptographic keys and verification of the identity of individual entities, which will differ from the procedures described herein. The modified procedure, which shall be adapted to the conditions of the emergency and thus cannot be further specified, must be in writing, approved by the PMA, assessed by the conformity assessment body and must not contravene Regulation (EU) No 910/2014 and national legislation, and may only be used for the duration of the emergency. After the end of the emergency, the procedures set out here must be followed.

3.2.1. Method of proving ownership of the private key

To issue or renew a certificate, the Provider receives an electronic request in PKCS#10 format. The specification of this certificate request format requires the request to be signed by a Signer who possesses the private key. The Provider verifies the validity of the electronic signature/seal accompanying the request. Demonstration of the validity of the affixed electronic signature/seal shall be sufficient reason to assume that the Signatory has submitted an electronic application and possesses a private key that is technically appropriate and corresponds to the public key specified in the application.

In case of a request for the issuance of a remote AdC electronic signature/seal, the Provider shall provide the Signatory with a remote service by generating a key pair in an encryption module that meets the requirements of a secure signature creation device.

In no event shall any component of the Provider archive any private keys belonging to the Holder of a AdC issued by the Provider. The only exception is private keys managed by the Provider for third parties in the framework of the provision of the data management service for the execution of an electronic signature or electronic seal on behalf of the signatory (issuer) (see Annex II of the eIDAS Regulation).

3.2.2. Legal entity identity authentication

Verification of the identity of the legal entity can be carried out at the RA's registered office and remotely at any location by signing the application for issuance of the AdC, by means of advanced electronic signature certificates of all managing directors, issued in accordance with paragraph 1 (a) or (b) of Article 24 of the eIDAS Regulation. The list of managing directors is obtained from the electronic extract from the commercial register valid for legal transactions, which the Client must provide, for example, via the slovensko.sk portal. Subsequently, all signatures are validated, thereby verifying the validity of signatures, the validity and authenticity of data and the validity of identification documents.

Legal entities that cannot be subject to automated verification should submit:

- a judgment or other document certifying the formation of the legal entity,
- any document attesting to their good condition, assessed by the RA,

- a unique national identifier.

The RA employee will then check whether the data provided in the AdES signatures and in the certified electronic extract from the commercial register or other statutory register match the data provided in the zone.nfqes.com application and in the application for the issuance of the certificate.

If the certificates are valid, the electronic extract from the commercial register (or other statutory register) is valid and the data in the Application, the certificate application, the extract from the commercial register (or other statutory register) and the data in the AdES signature are identical, the legal entity is authenticated.

For the issuance of an enhanced certificate for a natural person who is authorized by a legal entity, the authorized representative shall appear before the RA. Verification of the information contained in the documents submitted shall be carried out by the RA through:

- Certifications “true to the original” with the handwritten signature of the person concerned on the documents issued by the RA officer, in case of personal presentation of the documents by the authorized representative and signature of the authorized representative in front of the RA officer.
- Notarization of documents that are sent by e-mail to the RA.
- Signature of the attached electronic document formats by an authorized representative, with a valid advanced electronic signature/seal certificate.
- By checking and confirming using the Provider's application available at https://zone.nfqes.com.

Verification of the identity of the legal entity is to demonstrate that the legal entity exists when the application is examined and that the agent applying for the advanced certificate has the authority to apply for the advanced certificate on behalf of the legal entity. The RA employee may verify the registration through all available public services in accordance with Slovak legislation.

Verification of the identification or identity of a legal entity may also be carried out using an external information system managed by an external RA, provided that the data in this system is sufficiently verified in accordance with Regulation (EU) No 910/2014, the RA Operator has been informed of all identity verification procedures and the RA Operator agrees to provide such identity.

3.2.3. Authentication of the identity of a natural person

Identification and verification of the identity or identification of the natural person (Signatory) is carried out by the RA. Verification of the identification of the natural person may be carried out at the RA's registered office or remotely.

To identify and verify the identity of a natural person, proof of identity must be presented. The natural person requesting the issuance or administration of the AdC shall complete and submit documents to the Provider in accordance with the Provider's policy for the issuance and administration of AdCs. Personal data may include mobile phone number, email address, permanent address, etc.

Verification of the identity of the natural person can be done by means of an advanced certificate for advanced electronic signature, by which the natural person signs and agrees to the GTC and the natural person signs the application for the issuance of a certificate according to the CP.

In both cases (both at the RA headquarters and remotely), this perfected signature is validated, thus verifying the validity of the signature, the validity and authenticity of the data and the validity of the identification documents.

The RA will then check that the information provided in the AdES signature matches the information provided in the zone.nfqes.com application and the certificate application.

If the certificate is valid and the data in the Application, the Certificate Request and the data in the AdES Signature match, the natural person is authenticated.

The natural person confirms the authenticity of the data as follows:

- By handwritten signature on the documents in front of the RA officer, when presenting the documents in person.
- Notarisation of documents sent by RA e-mail.
- By signing the attached electronic documents with a valid advanced electronic signature certificate in accordance with Regulation (EU) No 910/2014.

The Provider shall verify the authenticity of the information in the completed documents by any means permitted by law. A list of documents required for the natural person to issue and manage an advanced certificate is provided in this policy.

Verification of the identity of a natural person may also be carried out using an external information system under the management of an external RA, provided that the data in this system is sufficiently verified within the meaning of Regulation (EU) No 910/2014, the RA Operator has been made aware of all identity verification procedures and the RA Operator agrees to the provision of such identity.

3.2.4. Unverified applicant information and specific attributes

All items on the advanced certificate must be verified. Any information beyond the mandatory verification is unverified information.

The Provider may include specific attributes associated with the Signer in the issued certificate if the certificate is issued for a specific purpose under the relevant policy. This information is subject to verification by the RA.

3.2.5. Validation of authority

Upon successful identification and verification of the conditions for issuing or managing an advanced RA certificate, the RA representative shall validate the data to the CA. The CA shall immediately publish the issued certificate in the certificate registry or the maintenance information in the CRL.

At brainit.sk, this certificate can only be revoked by the NFQES ACA Certification Authority that issued the advanced electronic signature/seal certificate or other trusted system.

See point 3.2.3.

3.2.6. Interoperability criteria

Improved certificates issued by the Provider meet the requirements of Regulation (EU) 910/2014 and are recognized in the European Union. Due to the cross-border interoperability of the formats of enhanced electronic signatures and seals introduced by Regulation (EU) No 910/2014, the advanced certificates do not exceed the mandatory requirements of Regulation (EU) No 910/2014. At national level, the enhanced certificates shall include specific data such as the national identification number and other specific data at the request of the user, but the Provider shall ensure that they do not hinder the cross-border interoperability and recognition of advanced certificates and electronic signatures/seals in the European Community.

3.3. Identification and authentication for key rekey requests

The Provider may renew a validly upgraded certificate that has not been terminated during the validity period by generating a new key pair ("Re-Key").

The Provider does not provide the option of recovery with the existing key pair or serial number preserved.

Issuing a subsequent AdC means changing the AdC key pair - a new AdC will be created, which will have the same distinguished name as the original, but the new AdC will have a different public key (corresponding to the new, different private key), a different Serial Number, and may have a changed validity length. This renewal of the current certificate with the new key pair is only possible if there have been no changes to the already authenticated information.

The customer requesting a subsequent AdC must submit to the requirements imposed on the initial registration (in particular, authentication of his identity).

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

When renewing the AdC, the provider shall comply with the following time limits and identification requirements:

Period / Period	**Renewal / Renewal**	**Requirements / Requirements**
Within 30 days prior to the expiry of a AdC that has not been terminated and that has no change in the data certified therein.	Re-key (Re-key)	• The certificate does not change • The renewal request can be made remotely
Within 30 days after the expiration of a AdC that has not been terminated and there has been no change in the data certified therein.	Re-key (Re-key)	• The certificate does not change • Renewal application can be made on the spot (in RA)
More than 30 days after the expiry of the AdC.	It is not renewed	

In the case of issuing and restoring AdC remotely using the application, the restoration is always Re-key. In this case, identity and identification checks are not performed, but identity verification checks are performed.

3.4. Identification and authentication in case of certificate termination

The request for revocation of a AdC must be authenticated, see paragraph 4.9.

A request for revocation of a AdC may be authenticated using a private key belonging to the AdC to be revoked, regardless of whether the private key has been compromised.

If the Provider terminates an advanced certificate, it shall reflect this in its databases as soon as possible after receipt of the request. The revocation shall take effect immediately after its publication.

The Provider shall terminate the Certificate only after successful identification and verification of the identity of the Signer and the specific reason for termination.

3.5. Identification and authentication after completion of the enhanced certificate

The Provider's advanced certification services policy does not allow for renewal of an advanced certificate upon termination.

The signer of a terminated certificate may request a new certificate.

The Provider, through the RA, shall perform the initial identification and verification of the Signatory's identity if the Signatory requests a new certificate.

4. OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF THE CERTIFICATE

The Provider, through the RA, shall provide the following operational procedures for advanced certification services related to advanced electronic signatures/seals within the framework of the concluded contract for the provision of advanced certification services:

- Registration of an application for an advanced certificate
- Processing of the application for an advanced certificate
- Issuance of an advanced certificate
- Surrender of the issued advanced certificate
- Using a key-pair and an advanced certificate
- Renewal of an advanced certificate
- Expiry of the advanced certificate
- Advanced Certificate Status

The Provider, through the RA, shall allow the Signatory to terminate the Advanced Certification Services Agreement between them. The time in the systems associated with certificate termination shall be synchronized with UTC at least once every 24 hours.

The Provider shall provide operational procedures for advanced certification services applicable to advanced electronic signature/seal certificates as described in the Certificate Services Statement (CPS) of this policy.

4.1. Using an advanced certificate and key pair

4.1.1. Users

Users must use private keys and appropriate advanced certificates:

- in accordance with their intended purpose,
- only within the period of their validity.

The signatory is responsible for the use of the private key.

4.1.2. Relying Parties

Relying parties, including the operator in the RA, must use public keys and their respective certificates:

- in accordance with their intended purpose,
- only after checking their status and checking the electronic signature of the CA that issued the certificate,
- until the key is revoked/expired.

4.1.3. Using public keys and certificates

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

4.1.3.1. Use of the Subscriber's private key and certificate

The obligation of the AdC Holder in relation to the private key and the AdC 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 AdC to the public key with which it is paired,
- for a AdC that has not yet expired, immediately notify the Provider if it suspects that:
    - their private key has been lost, stolen or compromised,
    - lost control of the private key by compromising their login credentials (password, mobile app or OCRA token),
    - inaccuracies or changes in the content of the certificate,
    - immediately request the revocation of the AdC if any information contained in the subject AdC has become invalid,
- refrain from using a private key and AdC that has expired, been revoked or compromised (including if the Provider itself has been compromised and the Holder/Customer is aware of this),
- comply with all terms, conditions and restrictions imposed on the use of your private key and AdC, such as discontinuing the use of your private key upon expiration or revocation of the AdC public key,
- use the AdC provided only for the relevant purposes recommended in this CP,
- immediately stop using the private key after it has been compromised.

4.1.3.2. Use of the relying party's public key and certificate

The relying parties are obliged to:

- establish a trust relationship with the CA that issued the AdC by verifying the certification path in accordance with the X.509 version 3 standard and the mandatory use of the trusted list of the country in which the issuer resides, as specified in the countryName entry of the issuer's name in the qualified certificate,
- store the original signed data, the applications necessary to read and process that data, and the cryptographic applications necessary to verify the advanced electronic signatures of that data, insofar as it may be necessary to verify the signature of that data.

4.2. Renewal of an advanced certificate

The provider shall not issue a AdC on a public key on which it has already issued a AdC in the past. Renewal of a AdC means the replacement of a valid certificate with a new certificate without changing the existing information contained in the certificate, except for a new serial number and a new validity period. Renewal shall only be done within the validity period of the current certificate. Prior to renewal, there shall be a record of the certificate renewal request in a suitable form accepted and approved by the RA operator. Identity and accuracy must be verified against the application submitted.

Renewal of an advanced certificate may be requested by the Signatory or an authorized person within the terms, requirements and conditions for renewal.

Advanced certificate renewal retains the Signer or Authorized Signatory information from the current certificate, where the validity period and serial number are changed in the renewed certificate.

Renewed certificates that have not been terminated during the validity period can be renewed by generating a new key pair (Re-key). The provider does not maintain the option of renewal with retention of the existing key pair or with retention of the serial number.

Renewal of an advanced certificate is preceded by registration of the renewal application with the RA or online.

When the AdC expires and the renewal application is within the specified timeframes and requirements for renewal identification, the Signatory or authorized person will visit brainit.sk's RA or perform the remote identification.

The certificate of the advanced electronic signature/seal may be repeatedly renewed by the Signatory or an authorized person. The Provider shall not allow the use of a key pair for an electronic signature/seal for a period longer than 3 years (unless contractually agreed otherwise).

The RA will restore the AdC of the electronic signature/seal using the Re-key under the following conditions:

- the certificate is not terminated during its validity period,
- the signer or authorized signatory declares that there has been no change to the certified data in his/her current certificate,
- an application for renewal of an advanced certificate shall be made within 30 days before the expiry of the validity period of the certificate,
- consistently performs user identification and authentication as well as meets the renewal deadlines.

In all cases when the certified data for the Signatory or the authorized person of the current certificate is changed, it is not renewable and brainit.sk will issue a new AdC.

An application for renewal of an advanced certificate shall include, as a minimum:

- the unique name of the Signatory or authorized signatory,
- type/designation AdC,
- the identifier of the authentication policy of the AdES certification policy under which the certificate is issued.

Some or all the data contained in the AdC renewal request may be verified by electronic signature/seal provided that the participant has a valid private key to create the signature/seal at that time. The Provider does not allow changing the certificate profile of the electronic signature/seal.

4.2.1. Issuance of a subsequent certificate

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

4.2.2. Terms and conditions for issuing a subsequent certificate

No provisions.

4.2.3. Who can apply for a follow-up certificate

A subsequent AdC 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.

4.2.4. Processing requests for the issuance of a subsequent certificate

The subsequent AdC must be issued in the same way as the original AdC was issued.

4.2.5. Notification of issuance of a subsequent certificate

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

4.3. Issuance of an advanced certificate

The detailed procedure is described in the CPS document of this policy.

Submission of an Advanced Certificate Request is the process by which a User submits a request for the issuance of an RA Provider's Advanced Certificate in written or electronic form under the relevant Certificate Issuance Policy. The request may be made by the Signatory or an authorized representative.

The user registers a request for an advanced certificate online or through an operator at the RA of the Provider. In online mode, requests are sent via network protocols such as HTTP/HTTPS, S/MIME or TCP/IP.

4.3.1. Who can apply for a AdC

The provider may be asked to issue a AdC:

- **AdC for advanced electronic signature**
  - a natural person or a natural person authorized by the Holder or a person acting on its behalf based on the law or a decision of a competent authority
- **AdC for advanced electronic seal**
  - any entity (the Customer) that, under applicable national legislation, has the authority to act on behalf of the legal entity in question

4.3.2. Registration process and responsibilities

The Customer must take the following steps in preparation for the visit or online meetings with the Provider, if a meeting is required:

- 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.com),
- familiarize yourself with the procedure and, where appropriate, the principles and guidelines for obtaining a AdC,
- prepare the values of the individual items of the AdC request so that these values are consistent with this CP,
- prepare your chosen identity documents or other necessary documents,

- in case of registration by RA, make an appointment.

4.3.3. Procedure before issuing the AdC in person

Before issuing the AdC, the employee representing the Provider must:

- inform the individual about the GTC, CPs and information on the management of personal data
- 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 IS of the Provider,
- verify all other documents submitted according to the established procedures.

4.3.4. Generating a AdC request

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

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

The application for registration of users of advanced certification services shall be submitted to the RA by natural person, legal entity or authorized persons and shall contain the following information:

- the full name of the Signatory or authorized signatory,
- proof of the Signatory's power of attorney over the author and the author's authorized signatory,
- UIC (Unique Identification Code) identifier,
- the person's postal address (country, district, postcode, city or town, building number, street name),
- e-mail address,
- the type of advanced certificate required, considering its designation,
- the identifier of the authentication policy under which the certificate is issued,
- the presence of a private key corresponding to the public key,
- public key,
- additional information that may be included in the certificate,
- signed contracts for advanced certification services and agreement to the terms and conditions of the policies and procedures for the provision of advanced certification services by brainit.sk.

Depending on the content of the certificate and its type, some of the above information may be missing.

If the cryptographic key pair is generated by the Signer, the RA shall check the submitted electronic registration request and the security level requirements of the device to generate the secure signature. Upon successful identification, verification of the identity of the person requesting the advanced certificate and receipt of the RA's acknowledgement, the registration request is sent to the CA for certificate issuance.

4.3.5. Submitting a certificate application

The request may be sent by technological interconnection of the two systems, if the interconnection, authorization and identification of the Holders is sufficient and if the Provider agrees to it, or by using the Provider's application.

In the case of use of the Provider's application, it is only made available to the RA worker after authorization using a name, password and a second factor, while the confirmation of the request and the subsequent processing of the request is also confirmed by a forced authorization by the RA worker. Once the request has been processed in zone.nfqes.com, all authorizations are then transferred to the person for whom the AdC is being issued, while complying with all provisions applicable to activation data.

4.3.6. Processing a certificate application

4.3.6.1. Processing user certificates

By signing the Certification Services Agreement or accepting the AdC applications, all AdC users accept the obligations and warranties contained therein and this policy. Each AdC user goes through a registration process that includes the following steps:

- applying for an advanced certificate that contains true and accurate information. The application may contain additional, unverifiable information, some of which is certified and some of which facilitates contact between brainit.sk and the Signatory,
- generation of the cryptographic pair key by brainit.sk or by the user himself,
- the electronic format of the application for an advanced certificate with the data to be contained in the certificate shall be the structure signed by the private key of the generated key pair on the secure signature/seal creation device,
- if necessary, the RA shall provide the Signatory or his/her designee with the information/code to access the private key on the secure signature/seal creation device in a protected form,
- in the case of remote generation of the pair key by the user, the user provides the public key to brainit.sk via RA and demonstrates ownership of the corresponding private key corresponding to the public key,
- based on approved applications for the issuance and management of an improved certificate, a contract is signed with brainit.sk.

4.3.6.2. Registration and Certification Authority Certificates

RAs providing improved services that are not in the organizational structure of brainit.sk (external RAs) are obliged to conclude an appropriate contract with brainit.sk before carrying out this activity. In addition to the rights and obligations of both parties, the contract should also specify the identity of the persons involved in the RA and their authority to represent both parties in the performance of the contract. Persons authorized to perform this activity shall define the type and designation before issuing certificates.

CA keys and certificates can only be generated during the key generation process, in which only persons authorized by brainit.sk participate.

4.3.6.3. Performing identification and authentication functions

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

Once the authentication and identification of the AdC Holder has been carried out and the required personal data has been entered into the Provider's system, the RA must enter the AdC application data and, in the case of the use of a pre-sent electronic application, ensure that the data is correct in the system.

4.3.6.4. Approval or rejection of certificate applications

The Provider shall not issue the AdC 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 with which the request was signed.

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

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

If for some reason a AdC cannot be issued for a given request, the RA employee must inform the Customer of this fact.

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

4.3.6.5. Time to process a certificate application

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

4.3.7. CA actions during certificate issuance

After sending the request for the issue of a AdC from the RA to the Provider's system, the Provider must perform a verification of the received request to verify that:

- was sent by an authorized RA,
- conforms to the PKCS#10 standard.

The issuance of a AdC on a key pair generated directly on the RA shall be securely bound to the procedure of this generation.

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

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 AdC 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 AdC Holder must be met when issuing such AdC.

4.3.8. Notification by CA to the applicant of the issuance of a certificate

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

4.3.9. Download certificate

4.3.9.1. Behaviour that constitutes acceptance of a certificate

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

4.3.9.2. Publication of the certificate

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

4.3.9.3. Notification of CA certificate issuance to other entities

No provisions.

4.4. Change of the improved certificate

Changing the AdC means changing the data content of a previously issued and published advanced electronic signature/seal certificate. After changing the AdC, a new key pair needs to be generated.

A change to the AdC is treated in the same way as the issue of a new AdC, and all defined procedures for issuing a new AdC must be followed.

The Provider does not support the release of a new AdC without changing the key pair due to changes related to its content.

4.5. Suspension and termination of an advanced certificate

The detailed procedure is described in the CPS document of this policy.

4.5.1. Circumstances of completion of the advanced certificate

The Provider shall terminate the AdC it has issued when the binding between the Signer and its public key in the certificate is no longer considered valid. The Provider shall terminate the AdC it maintains in the following cases:

- if the information on the certificate has changed and become outdated,
- if it is suspected that the private key associated with the public key contained in the certificate has been compromised,
- the user decides to terminate the contract with brainit.sk,
- learns that the Holder of the AdC has died, if it is a natural person or if it is a legal entity has ceased to exist,
- termination of the Signatory's representational authority over the Creator,
- the certificate revocation is requested by the AdC Holder,
- finding that the requirements of the eIDAS Regulation or Act No. 272/2016 Coll. were not met when issuing the AdC,

- finding that the AdC was issued based on false data,
- discovers that a private key belonging to a given AdC has been compromised, e.g. if access to a private key belonging to a public key listed in the AdC is known to a person other than the Holder listed in the AdC,
- the revocation of the AdC shall be ordered to the Provider by a court decision,
- the Holder has breached its obligations under this CP and/or the GTC,
- becomes aware that the Holder has become incapacitated by a court order,
- the Provider's private key has been compromised,
- if CA ceases to operate,
- if the user owes outstanding fees for the provision of advanced certification services.

4.5.2. Advanced Certificate Completion Procedure

The detailed procedure is described in the CPS document of this policy.

The process of terminating an upgraded certificate is preceded by a request to terminate the certificate. The request for termination of the AdC shall be made by the Signer or Authorized Signatory on-site at the RA or electronically remotely. At the time of termination of the AdC, the RA shall inform the user of this fact (e.g. by e-mail).

The Provider shall immediately terminate the operation of a valid certificate issued in each of the above circumstances. The Provider shall revoke issued certificates if it ceases to operate without transferring them to another Provider. In this case, it shall notify its users and terminate the certificates with one month's notice. Within one month of the notification, brainit.sk shall refund the amount paid by the users in the amount corresponding to the remaining period of validity of the advanced certification service contract. The Provider may suspend and terminate the CA if there are reasonable grounds for compromising the CA's private key.

The termination of the certificate of the operating CA for issuing and maintaining the AdC for advanced electronic signature/seal shall terminate the validity of all certificates issued and valid by it. This certificate can only be revoked by the functional CA that issued the advanced electronic signature/seal certificate. If the termination occurs due to operator error or due to a compromise of the operational private key of brainit.sk, the Provider shall issue an equivalent user certificate at its own expense.

Management, termination and suspension services are available 24 hours a day, 7 days a week. In the event of a system or service failure or other factors beyond CA's control, brainit.sk will use its best efforts to ensure service availability within three (3) hours.

4.5.2.1. Who can apply for certificate revocation

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

He may also request the revocation of his certificate:

- **The provider** - the employee in question is obliged to document this fact, including the reason for his/her action,

- **Subject** - (natural person or legal entity) based on the inheritance procedure (the Provider must attach to the documents on the revocation of the AdC a copy of the documents from which the right of the subject to apply for the cancellation of the AdC 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 revocation of the AdC),
- **a person authorized by the court**, e.g. the guardian of the AdC entity to be dissolved (a copy of the relevant court decision must be attached to the documents on the dissolution of the AdC by the Provider).

4.5.2.2. Procedure for requesting revocation of a certificate

Revocation of the AdC must be requested by the authorized person in person at the Provider or remotely by technology. The person requesting revocation of the AdC must undergo the same authentication process with the Provider as is required for the initial registration of the Holder/Customer (see paragraph 3.2) or must present an agreed password for revocation of the AdC, which the Holder/Customer may receive after the AdC has been issued, or the request must come from a system trusted by the Provider.

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

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

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

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

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

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

A request for certificate revocation may also be made in writing. The holder/customer must specify in the written request the serial number of the AdC whose revocation is requested and must authenticate the revocation using a valid password for revocation of the AdC.

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

4.5.2.3. Time to apply for cancellation of the AdC

In the event of a threat of compromise of the private key, the authorized person must submit a request for revocation of the AdC as soon as possible. In-person revocation may only be requested during the time specified by the RA. For electronic requests, this can be sent to the internal RA at any time.

4.5.2.4. Time within which the CA must process the cancellation request

The provider must:

- revoke the AdC without delay and no later than 24 hours after verification that the request for revocation is justified,
- publish the current list of revoked AdCs and all previous lists of revoked certificates so that they are accessible to Customers/Holders and all relying parties,
- inform the Customer/Holder of the revocation of his/her AdC by sending an e-mail to the e-mail address provided by the Holder during the registration process for RA, including the reason for the revocation of the AdC,
- 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.

4.5.2.5. Cancellation control requirement for relying parties

The relying party is obliged to verify the validity of the AdC by means of an available CRL or OCSP service when relying on the AdC.

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

Failure to validate the AdC using a CRL or OCSP is considered a gross violation of this CP.

4.5.2.6. Frequency of issuing CRLs

The provider shall, as far as possible, immediately publish a CRL whenever a valid certificate issued by this CA is revoked.

The requirements for the frequency of issuing CRLs are as follows:

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

4.5.2.7. Maximum latency for CRL

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

The Provider must ensure that each CRL is published immediately after it is created, but no later than 60 minutes (1 hour) after the new certificate is added to the CRL.

4.5.2.8. 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.

4.5.2.9. OCSP control requirements

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

4.5.2.10. 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, available at: https://zone.nfqes.com/crl/
- the Provider must ensure that a telephone or e-mail enquiry regarding the status of a particular certificate is answered.

4.5.2.11. Special requirements for changing keys after they have been compromised

In the event of a breach of the private key security (its disclosure) by the CA or other entities operating within the Provider, the Provider will immediately inform the relying parties.

4.5.2.12. Circumstances in which the validity of the AdC is suspended

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

4.5.2.13. Who can apply for suspension of the AdC

No provisions.

4.6. Services related to certificate status

4.6.1. Operational requirements

The list of revoked certificates shall be available at the URL of the Provider and shall be accessible via HTTP protocol on port 80.

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

4.6.2. Service availability

Service availability is in 24/7 mode at an SLA level of 95%.

4.6.3. 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 AdC, he/she must also apply for revocation of the certificate.

5. PHYSICAL, PERSONNEL AND OPERATIONAL SECURITY MEASURES

This section of the policy describes the general requirements regarding physical and organizational security controls, as well as personnel operations used at brainit.sk. It reviews security requirements and procedures at the time of key generation, customer identification and identity verification, issuance and management of advanced certificates, auditing and archiving.

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 measures taken regarding to the Provider's physical security are part of the Provider's information security system, which meets the requirements of ISO/IEC 27001, ISO 9001, ISO 22301.

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

Measures relating to the physical protection of information data, technology systems, premises and related support systems shall be designed to prevent breaches:

- the Provider shall control physical access to objects whose security is essential for the provision of trusted services and minimize any risks associated with physical security. The security of the systems for issuing and managing certificates shall comply with the requirements of international standards and recommendations,
- physical access to the components of the Provider's system, the security of which is essential for the provision of trusted services, is limited to authorized persons only. The criticality of the components shall be identified by a risk assessment. Physical integrity is ensured with respect to equipment located in protected and isolated areas. Two-factor access control and 24/7 physical security is in place. No physical access to critical equipment is allowed for more than 30 minutes per visit. No more than 2 authorized

Provider technical personnel shall have access to the equipment cabinet. Any access to critical infrastructure areas shall be documented and maintained in logs,

- the control shall be applied for the purpose of preventing loss, damage or endangerment of property and interruption of business. Authorized Provider personnel shall strictly adhere to internal procedures for access to the various restricted physical access areas,
- controls shall be applied to prevent data compromise or theft of information processing tools. The physical security of the premises located the core infrastructure is ensured by their solid, stable construction with strong doors and key locks,
- the Provider shall configure its systems by removing or disabling all accounts, applications, services, protocols and ports that it does not use in its operations,
- the provider shall only grant access to protected and high security areas to trusted roles,
- the Provider's ACA system is in a high security zone. The Provider's primary CA is in a certified data center.

Brainit.sk provides physical protection and access control to areas where critical components are installed in the infrastructure:

- Qualified Root CA - CA Signing Certificate
- Qualified Operating CA - NFQES ACA,
- Qualified OCSP service for verifying the status of certificates issued by a basic and operational authority (OSCP service) - CA OCSP Signing Certificate,
- TSA Qualified for Time Certification - NFQES TSA,
- Registers and provider's website,
- Registration authorities,

The Provider's infrastructure is physically and logically separated and is not used for other activities carried out by brainit.sk.

5.1.1. Premises

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

5.1.2. Physical access

The physical security of the certification and management systems complies with the requirements of international standards and recommendations.

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 granted to persons who possess a security token and are listed on the list of persons authorized to enter the Provider's protected premises. The Provider's equipment must be always protected against unauthorized access, including unauthorized physical access. Any entry of other persons must be always recorded and may only be permitted when accompanied by an authorized person.

5.1.3. Power supply and air conditioning

The premises in which the Provider's equipment is located 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, 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 Safeguards - Organisational Control

All security procedures for the issuance, management and use of the AdC for advanced electronic signature/seal shall be performed by trusted personnel of the Provider.

Brainit.sk has enough qualified employees who are able to ensure compliance with applicable legislation, internal company rules and regulations always.

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.

The Provider has a detailed definition of the division of functions and responsibilities of the staff (*Provider's internal documents: job description, job plan and relevant internal documents*).

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.

The allocation of functions shall be carried out to minimize the risk of compromise, leakage of confidential information or conflicts of interest.

5.2.2. Number of persons required for the task

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

5.2.3. Identification and authentication for each role

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

5.2.4. Roles requiring division of responsibilities

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

5.3. Personnel security measures

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

The Provider's staff shall consist of a sufficient number of highly qualified employees. Trusted persons shall have the necessary training and experience to ensure these security requirements and technical security assessment standards. They shall have the knowledge of information systems, cryptography and PKI to properly perform their duties.

5.3.1. Qualification, experience and vetting requirements

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

5.3.4. Training renewal frequency

For roles where there are requirements to complete prescribed training, the need for refresher training after the primary training can be established.

5.3.5. Roll rotation frequency

No provisions.

5.3.6. Penalties for unauthorized conduct

The failure of any employee of the Provider to comply with the provisions of this CP or the adopted CPS, whether intentional or negligent, 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 action by an employee in a trusted role identified by Provider management must result in immediate removal from the trusted role pending completion of the ongoing management review. After the 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.

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 for as long as necessary, even after the activity has ceased, all relevant information relating to the AdCs 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.

For the effective management and operation of the Provider, all events that have a significant impact on the safety and reliability of the technology system, personnel and user control and the security impact of the advanced certification services provided shall be recorded.

The information in the electronic logbook is generated automatically and records of recorded events are stored in files on the system disk until at least the completion of the next periodic external audit.

The provider shall classify and maintain registers of all assets in accordance with ISO/IEC 27001. According to the Security Policy of brainit.sk, an analysis is performed to assess the vulnerability of all internal procedures, applications and information systems. The analytical requirements may also be determined by an external institution authorized to audit the Provider. The risk analysis shall be performed at least once a year.

5.4.1. Types of recorded events

The provider must record and evaluate the following important events:

- processes related to the Provider's key lifecycle (generation, backup, recovery, destruction, etc.),
- data obtained during the provision of 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 obliged to continuously monitor the sent system logs to detect potential threats to the provision of the Provider's services in a timely manner. All recorded logs in electronic form must be stored on recording media at regular intervals, at least 1 time per month, so that they can be made available to auditors. Similarly, all written audit trails of processes related to the key lifecycle of the Provider's Certification Authorities, 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 premises.

5.4.5. Audit log backup procedures

No provisions.

5.4.6. Audit collection system (internal vs. external)

No provisions.

5.4.7. Notification of the entity initiating the audit

No provisions.

5.4.8. Vulnerability assessment

See point 5.4.2.

5.5. Archive records

Information on significant events is regularly archived electronically. The Provider backs up all data and files related to: registration information, system security, all requests submitted by Users, all User information, all keys used by Certification Authorities and Registration Authorities, all correspondence between the Provider and Users. All documents and data used in the authentication process shall be subject to archiving.

The provider shall store the records/logs in a format allowing reproduction and retrieval.

5.5.1. Types of archived records

The provider must keep all records of issued AdCs as well as the AdCs themselves in accordance with the requirements of the legislation currently in force for the period specified in clause 5.5.2.

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 AdC application together with the relevant documents confirming the identity of the Holder in paper or electronic form for at least 10 years from their creation.

5.5.3. Archive protection

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

5.5.4. Archive backup procedures

The ability to fully restore backups (e.g. after a system failure) is essential for the proper functioning of the Provider.

Detailed procedures for archiving, making copies and restoring the system after accidents are described in the Provider's internal documentation, which is accessible only to authorized personnel.

5.5.5. Time stamp requirements for records

Archival records are secured by a time-stamp of their creation.

5.5.6. Archiving system

The archive data collection system is an internal system of the Provider. An exception to this rule is archives collected by the RA. Archival information (on paper and on electronic media) shall be properly stored and subject to a high level of physical security.

5.5.7. Procedures for obtaining and verifying archival information

Access to the archive is only possible for authorized persons. The data shall be regularly checked and compared with the original data to verify the integrity of the archived information. This activity shall be supervised by the Security Administrator. If corruption or alteration of the original data is detected, the damage shall be repaired as quickly as possible in accordance with the Provider's internal procedures and policies.

5.6. Key change

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

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

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

The Provider may only change the key corresponding to an issued certificate by issuing a new certificate or by renewing the current certificate.

The private key of the CA can be changed if:

- the expiry of the accompanying certificate,
- the introduction of new services by the Provider that entail changes in the characteristics of the private key (for example, security-related changes and the requirement for new usable cryptographic combinations).
- in case of a change of the private key of the Provider's CA, the following rules shall be observed:
    - the CA whose key the user certificates are signed with and whose key is to be modified shall suspend the issuance of certificates 60 days before the point in time at which the remaining validity period of the private key equals the validity period of the last issued certificate,

- a CA whose private key is signed by a CRL and whose private key will be changed shall continue to publish CRLs signed with the old private key until the last published certificate expires.

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

5.7.2. Computing resources, software or data are corrupted

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

5.7.3. Private key compromise procedures

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

5.7.4. Maintaining business continuity after a disaster

The provider must have procedures in place to ensure business continuity in the event of an emergency due to, for example, a natural disaster, to ensure its ability to resume operations. The procedures must include the location of 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 activity 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.

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

- give at least 6 months' notice in an appropriate manner, where practicable, of the planned termination of its activities to the Supervisory Authority, the Holders of any valid AdCs issued by it, parties relying on the AdCs 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),
- to cancel all valid AdCs before ceasing operations if it fails to ensure continuity in the provision of its services,
- attempt to contract with another qualified trust service provider to ensure continuity in the provision of its advanced 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 to the processing of personal data and on the free movement of such data and Act No. 18/2018 Coll. on the protection of personal data,
- disable all private keys, including copies thereof, in such a way that they cannot be recovered in any way.

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

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

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

6. TECHNICAL SAFETY MEASURES

This section describes the procedures for generating and managing cryptographic keys and the associated technical requirements. The Provider shall only use reliable and secure hardware and software that are part of the Provider's computer system. The computer systems on which all critical infrastructure components operate shall be equipped and configured with tools to locally protect access to software and information data. The Provider applies information security management procedures for the entire brainit.sk infrastructure in accordance with generally accepted and international practices and standards.

To ensure the reliable operation and security of the computer systems lifecycle, the Provider shall carry out activities in accordance with the following requirements:

- When developing new systems, the Provider carries out an analysis of security requirements already at the design and specification stage, thus guaranteeing the integration of security into IT systems.
- The Provider shall implement a security policy and change control procedure during updates, modifications to emergency and operational software, and configuration changes.
- Procedures include documenting changes.
- The provider protects the integrity of systems and information against viruses, malware and unauthorized software.
- The provider shall develop and apply procedures for all trust and administrative tasks that impact service delivery.
- The provider shall specify and implement procedures to ensure that:
    - all available security and functional software updates are applied within a reasonable time after they become available,
    - protective and functional updates shall not be applied if they are likely to introduce additional vulnerabilities or instabilities that outweigh the benefits of their application,
    - the rationale for refusing to apply any security or functional updates is documented.

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 2.

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

Cryptographic key pairs for the Provider's operational certificates shall be generated and installed according to the instructions and procedures in the CP or CPS document.

The generation shall be carried out by authorized persons of the Provider in compliance with the requirements of at least dual control. A protection mechanism with a security profile created in accordance with the technical specifications defining the security levels shall be used to create the signature.

The Provider shall use its private keys only for the purposes of its business, as follows:

- sign the issued CA operational certificates in its infrastructure,
- sign issued and published CRLs,
- sign all issued and published electronic signature certificates/user seals.

The cryptographic key pair (private and public) of the electronic signature/seal certificates issued in the Provider's infrastructure is generated as follows:

- the signatory, with hardware and software under its control, but approved by brainit.sk,
- by the RA Operator of the Provider with hardware and software under its control, but approved by brainit.sk,
- Provider's RA operator with hardware and software under the control of Provider's infrastructure,
- by brainit.sk, when the certificate is requested remotely, through the Provider's application,

The signatory undertakes to use licensed software to work with the electronic signature/seal creation device.

6.1.1. Generating key pairs

The Signatory's AdC keys for the advanced electronic signature/seal shall be generated in a secure environment as required by Regulation (EU) No 910/2014.

The control of the private key is through the passcode. The signer uses the private key to create a signature/seal by entering a code in a secure environment to create an advanced electronic signature/seal.

When the key pair is generated by the Signatory, brainit.sk recommends that the Author uses an approved environment in the Provider's infrastructure to create an advanced electronic signature/seal or equivalent that meets the requirements of Regulation (EU) No 910/2014 and is compatible with the Provider's infrastructure.

In cases where a key pair is generated by a Signatory or Creator, the Signatory or Creator is fully responsible for protecting the private key to prevent its disclosure, publication, modification, loss or unauthorized use. The Signer is responsible for the omissions or actions of authorized persons who are authorized to create, store or maintain their private keys.

The signer agrees to use licensed software to work with the environment to create an advanced electronic signature/seal.

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 must provide sufficient confidence in the generation procedure. The entire process of the generation method shall be recorded. Key generation must be performed in a secure cryptographic key storage facility that meets the legislative requirements for this type of facility.

brainit.sk generates cryptographic key pairs at the company's headquarters and operational CAs using an HSM hardware security module at a minimum of FIPS 140-2 level 2 or higher.

6.1.1.1. Environmental requirements for the creation of an advanced electronic signature/seal

The environment for the creation of an advanced electronic signature/seal must ensure, by appropriate technical and procedural means, that at a minimum:

- the confidentiality of the data for the creation of the electronic signature/seal is adequately guaranteed,
- the data for the creation of an electronic signature/seal were practically fulfilled only once,
- the data on the creation of the electronic signature/seal is sufficiently secure and cannot be inferred with certainty and the electronic signature is reliably protected against forgery by currently available technology,
- the data for the execution of the electronic signature/seal must be reliably protected by the authorized Signatory of the signature/seal against use by other persons.

The Advanced Electronic Signature/Seal Creation Environment shall not alter the data to be signed or prevent such data from being presented to the Signer prior to signing.

The generation or management of data for the creation of an electronic signature/seal on behalf of the Signatory of the electronic signature/seal may only be performed by the Provider.

6.1.1.2. Remote key pair generation

The signer uses specialized software provided by brainit.sk, which implements the process of generating and managing the cryptographic key pair.

The generation, use and storage of a private key has a high level of security that is guaranteed by the environment where it is created. It is securely protected and accessible only to the Signatory or an authorized representative of the legal entity.

The signatory or authorized representative of the legal entity shall generate an electronic request for AdC in PKCS# 10 format and send it to the Provider. Following the recommendations of RFC 2314 - PKCS# 10, the electronic request form contains the DN, public key and other attributes, all of which are signed with the private key.

If on-demand remote key pair generation is performed, it shall be generated in a trusted Provider environment that meets the requirements and regulations for an advanced electronic signature environment.

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).

The length of the key pair for the advanced electronic signature/seal generated by the Customer through the Provider's infrastructure shall be at least 3072 bits, with a usable combination of asymmetric and hashing algorithms: sha256-with-RSA. Regardless of where the key pair is generated for the Advanced Electronic Signature/Seal Certificate, the key shall be at least 2048 bits in length for RSA and DSA algorithms and 160 bits for ECDSA algorithms.

6.1.6. Public key parameters and quality control

The quality and parameters of the Provider's public keys must be determined by the PMA. The established parameters must be respected during the key generation ceremony. The Provider shall use FIPS 140-2 Level 2 compliant cryptographic hardware modules for key generation and storage that provide random generation of RSA keys of at least 3072 bits in size.

For each type of AdC 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.

The signer or authorized representative of the legal entity of the key pair is responsible for verifying the quality of the generated private key parameters. The ability of the key to encrypt, decrypt and generate electronic signatures shall be verified.

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

Each user creates and stores a private key using a reliable system for their security. The CA generates a key pair and sends it to the user upon request, informing the user of the rules for storing and protecting his private key.

6.2.1. Cryptographic module standards and controls

The private key of the Signatory or the authorized representative of the legal entity shall only be used in a secure environment to create an advanced electronic signature/seal as required by Regulation (EU) No 910/2014.

The provider must use hardware cryptographic modules that are certified to FIPS 140-2 level 2 to protect the private keys of its issuing CAs. The modules must be stored in secure areas that can only be accessed by persons in trusted roles.

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 always be present on a "K" of "N" designated authorized persons basis (4 of 8)

6.2.3. Saving the private key

The provider does not store or archive in any way the user's private key for the creation of the electronic signature/seal.

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

See 6.2.3

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

The Provider's private keys, which are used in the execution of issued AdCs 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.

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

6.2.9. How to deactivate the private key

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

6.2.10. Method of destroying the private key

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

The public keys of the Signatories or authorized representatives of the legal entity are contained in the AdCs issued to them and published in the certificate registry on the User's website.

6.3.2. Certificate operating periods and key pair usage periods

The duration of public key use is determined by the value of the field in the certificate describing the validity of the public key. The validity of certificates and their corresponding private keys may be shortened if the certificates expire.

The validity of the improved certificates produced by the Provider and the usability of the key pair shall not exceed the following values:

Type of certificate	Validity (maximum)
Issuing CA	30 years
Issuing ACA	8 years
AdC for the end user	3 years

6.4. Activation details

When the User is present on the RA (in person or technologically via the system), the private key activation data is primarily used by the RA operator. Users use authentication and control access to their private key.

In cases where the Signatory or the legal entity's authorized representative generates the certificate's advanced key pair, the Signatory itself creates and manages the activation data.

6.4.1. Generating and installing activation data

The activation data is used during the initial issuance of the certificate in the environment to create the advanced electronic signature/seal.

The access codes and unblocking environment for the creation of the advanced electronic signature/seal shall be provided to the Signatory or the legal entity's authorized representative in a stamped and opaque paper envelope or in electronic form through an alternative channel.

AdC Holders' activation data (password, SMS token or mobile app or OCRA token) that are linked to a specific Holder must be handed over during the face-to-face meeting during the AdC issuance or online. The Holder must be advised of the method and need to change them and of the risks if they do not make the said changes. The activation data may be in the form of an S/N token, a PIN, a password or a password divided into several parts based on the k/n principle, etc.

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

6.4.2. Activation of data protection

Holders are solely responsible for the protection of their private access data, mobile applications and PINs to Holders' tokens.

A key pair intended for the AdC publisher:

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

6.4.3. Other aspects of activation data

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

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

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

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

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

6.5. Computer security checks

Brainit.sk uses only reliable and secure hardware and software that are part of the Provider's computer system.

Computer systems that operate all critical components of the Provider's infrastructure shall be equipped and configured with means of local software protection and information access.

The Provider shall use procedures to manage information security across its infrastructure with generally accepted international standards.

6.5.1. Specific technical requirements for cyber security

The provider shall perform all the functions of a qualified trust service provider using a trusted system that meets all the security requirements for the provision of trust services.

A provider issuing AdCs 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. Cyber security assessment

No provisions.

6.6. Measures and security in the life cycle

All hardware changes are monitored and registered by the Provider's authorized personnel. When new hardware is purchased, it is supplied with the necessary operating procedures and instructions for use. The functionality of the technological system is supervised and ensured to function properly and in accordance with the supplied production configuration.

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

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.

The Provider uses modern technical means of information exchange and protection to ensure network security of systems against external interference and threats.

6.8. Time stamp

The Provider shall use its own qualified time-stamps, which have the status of a qualified trust service provider and provide a qualified trust service for the creation of an advanced electronic time stamp within the meaning of the provisions of Regulation (EU) No 910/2014 (eIDAS). Certificate, CRL and OCSP processes.

6.9. Certificate Profile

AdC 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) can arbitrarily change the structure of these profiles or responses.

The structure of the AdCs produced by the Provider may only be changed based on a decision of an authorized member of the PMA.

Advanced certificate profiles shall conform to the format described in the X.509 version 3 standard. An X.509 version 3 type certificate is a set of data that uniquely authenticates the public key for the originator of an advanced electronic signature/seal.

6.9.1. Version numbers

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

6.9.2. 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 ()	Contents of individual headings for each type of AdC **C (countryName)** = **Country: the** two-character ISO 3166 country code of the nationality of the natural person as indicated in the identity document provided. **CN (commonName)** = **Full name**: The full name of the natural person in roman characters according to the identity document. **G (givenName)** = **First name**: The name of the natural person in roman characters according to the identity document. **S (surname)** = **Surname**: The surname of the natural person in roman characters according to the identity document.

	SERIALNUMBER (serialNumber) = National identifier of a natural person according to ETSI EN 319412-1, clause 5.1.3. Example: PNOSK-1234567890 *(birth number*) **dateOfBirth** = Date of birth expressed in ZULU format, for example: 19801220120000Z. **placeOfBirth*** = place of birth **gender** = sex of the natural person **stateOrProvinceName*** = current permanent address: name of the region, state or province **localityName*** = current permanent address: city name **streetAddress*** = current permanent address: street name, number or floor **telephoneNumber*** = mobile phone number **emailAddress*** = email address **Title*** = Occupation/position/profession **O** (organisationName)** = Name of the legal entity: full name according to the certificate of registration of the legal entity with which the natural person is associated **organizationIdentifier** = legal entity identifier according to ETSI EN 319 412-2, clause 5.1.4. Example: NTRSK-123456789 (PIN)
Public key	The public key for which the certificate is made (RSA, min. size 3072 bit)
Extensions	See Table 5 for a list of extensions in AdC

* - Fields marked with an asterisk (*) do not need to be included in the certificate

** - Fields marked with two asterisks(**) - attributes of the legal entity organizationName and organizationIdentifier are filled in only if the natural person is a representative of the legal entity. If no attributes for organisationName and organisationIdentifier are filled in, the attribute identifying the link to the legal entity (id-etsi-qcs-SemanticId-Legal) will be left blank.

6.9.3. 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
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 advanced 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 AdC for website authentication	No

6.9.4. Algorithm object identifiers

Signature Algorithm for signing of executed AdCs (Signature Algorithm)

sha256RSA OID: 1.2.840.113549.1.1.11

6.9.5. Forms of names

The first name(s) in the givenName (GN) field and the last name(s) in the Surname (SN) field must be entered in the AdC for the electronic signature. The first name(s) and surname(s) together in the form specified by the Holder/Customer shall still be entered in the commonName (CN) field.

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

For a Web site, the specified domain name (FQDN) must be specified in the CN field in the AdC for authentication of the Web site, as well as in the subjectAltName extension.

The issuing CA's certificate must always include the Provider identifier in the form "NFQES ACA".

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

Key lengths and validity AdC: Public key

- RSA, minimum length 3092 bits
- EC, minimum length 160 bits

6.9.6. Restrictions on names

No provisions.

6.9.7. Certification policy identifier

See chapter 1.2.

6.9.8. Using extensions to restrict the policy

This extension is not used.

6.9.9. Syntax and semantics of politics

Each AdC 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).

6.9.10. Extension

No provisions.

6.10. Profile of CRL

6.10.1. 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 shall comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

6.10.2. 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

6.11. Profile of OCSP

6.11.1. 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 AdCs, their signing certificates shall be signed by the corresponding Provider CAs and shall contain an extension to use the OCSP Signing key (1.3.6.1.5.5.7.3.9).

6.11.2. 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

7. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The audits carried out by the Provider concern the processing of information data and the management of key procedures. The Provider shall carry out at least one internal audit per year and shall be audited at least once every 24 months by a conformity assessment body.

The purpose of the audit is to confirm that the Provider, as a qualified certification service provider, meets the requirements set out in Regulation (EU) No 910/2014 or the requirements set out in the eIDAS Regulation.

7.1. Frequency or circumstances of assessment

The Provider shall be audited at least every 24 months by a conformity assessment body on the advanced trust services it provides.

7.2. 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 2.2.2.2 in accordance with the NBÚ certification scheme that governs the requirements of this standard.

7.3. 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.

7.4. Topics covered by the evaluation

The purpose of the audit is to confirm that the Provider as an advanced trust service provider and the advanced trust services it provides meet the requirements set out in Regulation (EU) No 910/2014 or the requirements set out in the eIDAS Regulation, as appropriate.

7.5. Measures taken as a result of the shortfall

Internal and external audit reports shall be sent to the Provider. Based on the evaluations set out in the report, the PMA shall establish appropriate measures and deadlines to remedy the shortcomings and irregularities identified. The Provider's staff shall take specific measures to remedy them within the time limits laid down.

When the auditor identifies a discrepancy between the Provider's operations and the applicable requirements or provisions of the CP and the 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.

7.6. 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.

8. OTHER BUSINESS AND LEGAL MATTERS

8.1. Fees

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

Fees for advanced trust services provided by the Provider shall be paid by the Customer, unless otherwise agreed with the Provider.

8.1.1. Fees for the issue or renewal of a certificate

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

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

8.1.2. Fees for access to the certificate

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

8.1.3. 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.

8.1.4. 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.

8.1.5. 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.

8.2. 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.

8.2.1. 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.

8.2.2. Other assets

No provisions.

8.2.3. Insurance or guarantee for end-users

No provisions.

8.3. Confidentiality of business information

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

8.3.1. 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 Provider's operation, including its RA, the Provider's private keys used for signing the executed AdC,
- OCSP responder private keys used to sign responses to requests to confirm the existence and validity of the AdC,
- personal data of Certificate Holders subject to protection under the Personal Data Protection Regulations.

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

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

8.3.2. 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 adoption by the other party, or subsequently become so 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.

8.3.3. 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 provided or disclosed to a third party in the performance of its activities for the Provider, the Provider shall enter into a confidentiality agreement with the third party, or a contract on the provision of confidential information, which also contains the above obligations.

The Provider may disclose certain confidential information to a third party in certain circumstances, in 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.

8.4. Privacy Policy

The Provider strictly observes the requirements for confidentiality and non-disclosure of personal data of the Customer/Holder or authorized representatives of legal entities with which it is familiar as a provider of advanced certification services.

8.4.1. Data Protection Plan

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

The Provider shall ensure the confidentiality and integrity of the personal data obtained in the process of issuing the enhanced certificate, 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:

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

8.4.2. 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.

8.4.3. 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 advanced trust services that are not considered personal data.

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

8.4.4. Responsibility for the protection of private information

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

8.4.5. 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.

8.5. Intellectual Property Rights

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

The various data included in the Provider's advanced certificates or published in the registry/repository are subject to intellectual property rights and other proprietary and intangible rights.

The user key pair and the corresponding public key certificate issued by the Provider, as well as the corresponding secret material, are the property of the Provider regardless of the ownership of the physical environment in which the keys are stored and protected.

8.6. Declarations and warranties

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

8.6.1. 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,
- fulfilling its obligations under Regulation (EU) 910/2014 and national regulations in the exercise of its activities as a qualified certification-service-provider,
- 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,
- the fact that the Holder becomes or is the owner of the Private Key at the time of execution of the Advanced Certificate under this CP,
- the accuracy of the information contained in the completed advanced certificates to the best of the Provider's knowledge and compliance of the issued advanced certificates with the requirements of the eIDAS Regulation,
- Compliance with the Data Protection Regulations in the handling of Holders' personal data,
- Issuance of advanced certificates for electronic signature/seal after verification of the information specified by law,
- termination or suspension of certificates under the terms and conditions described in this CP.

8.6.2. RA Declaration and Warranties

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

8.6.3. Declarations and warranties of participants

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

- generation of the public key/private key pair in case it generates the keys to the AdC request on its own,
- 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 in the Provider's repository and on its website (see Chapter 1),
- use of issued AdCs only for legal and authorization purposes in accordance with this CP,
- terminate the use of the AdC if any information contained therein proves to be misleading, outdated or incorrect,
- make every effort to prevent compromise, loss, declassification, modification or any unauthorized use of the private key corresponding to the public key contained in the AdC issued by the Provider.

8.6.4. 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.com/).

8.6.5. Representations and warranties of other participants

No provisions.

8.7. Disclaimer of warranties

The Provider shall be solely liable under Article 13 of the eIDAS Regulation for damage caused by the failure to fulfil its obligations under the eIDAS Regulation.

8.8. Limitations of liability

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

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

- breaches of obligations by the Certificate Holder/Customer or Relying Party set out in generally applicable law, the relevant contract, the GTC or the Provider's policies, including the obligation to exercise reasonable care in using and relying on the Certificates,
- failure of the Certificate Holder/Customer to provide the necessary cooperation,
- the technical characteristics, incompatibility, configuration, unsuitability or other defects of the software or hardware used by them,
- using or relying on a certificate that has expired or been revoked,
- use of the certificate by the Certificate Holder/Customer in violation of the Contract, the GTC or the Provider's policies,
- that the certificate has been used in violation of its designation, purpose or limitations specified in the certificate, in these GTC or in the Provider's policies,
- 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),
- failure to provide any of the trusted services or their unavailability during planned maintenance or reorganization announced on the Provider's website,
- the action of a higher power.

The Provider shall not be liable for damages incurred by the Relying Party due to its failure to follow Chapter 10 of the GTC and this CP when relying on the Provider's AdC and trusted services or on an advanced electronic signature or seal made on their basis. or the Relying Party information.

From the moment the Holder gains access to the private key to which the AdC belongs, the Provider shall not be liable:

- for the protection of the device on which the AdC and the private key are stored, or for the protection of the access codes necessary for its use,
- for the unauthorized person taking possession of the device or the private key,
- for damages caused using the private key or the AdC if the Holder/Customer does not act in accordance with his/her obligations, if the private key is seized by an unauthorized person and the Holder/Customer does not request the Provider to cancel the AdC or if he/she does not notify the Provider of changes in the data.

The liability of the Customer/Holder or the authorized representative of the legal entity arises from the performance of his/her duties. The terms of liability are governed by the contract with the Provider. The Customer/Recipient or the authorized representative of a legal entity shall be liable to the Provider and the relying parties if:

- used an algorithm and environment to create an advanced electronic signature/seal that does not meet the requirements of Regulation (EU) No 910/2014 when creating the private-public key pair
- it does not meet the security requirements set by the Provider
- does not request the Provider to suspend or terminate the AdC after becoming aware that the private key has been misused or compromised by improper use
- made false statements to the Provider regarding the content or issue of the AdC

The Customer/Recipient or the representative of the legal entity is responsible for the content of the attachments and the consequences of their use.

8.9. Compensation

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

8.10. Duration and termination

8.10.1. Deadline

This version of the CP is valid from the date of its entry into force, i.e. 1.1.2024, 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.

8.10.2. 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 1.1, or on the date of termination of the activity of provision of enhanced trust services by the Provider at the time of its validity. All revisions to the CP and CPS that are listed in the change history for the document must be made available to Holders/Customers and/or Relying Parties.

8.10.3. Termination and survival effect

If this document is not superseded by a new version and the Provider's provision of advanced trust services is terminated during the term of this document, 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 upon termination.

8.11. Individual notifications and communication with participants

The Provider's communication with the internal RA must be made officially via authorized e-mail communication between the Provider's designee and the RA's designee, unless otherwise specified in the contract.

8.12. Amendments

8.12.1. 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.

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

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

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

8.12.2. 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.

8.12.3. 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.

8.13. Dispute resolution provisions

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

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

In this case, he/she is entitled to contact the out-of-court dispute resolution entity, which is the Slovak Trade Inspection or another 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

Holder/Customer has the right to choose which of the aforementioned alternative dispute resolution entities he/she will 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.

8.14. Applicable law

Legal relations between the Provider and the Certificate Holder/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 in the Slovak language between the Provider and the Customer, the GTC and this CP shall be governed by the relevant provisions of Act No. 513/1991 Coll., Commercial Code, as amended, Act No. 40/1964 Coll., Civil Code, as amended, and other generally binding legal regulations of the SR.

8.15. Compliance with applicable legislation

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

8.16. Miscellaneous provisions

No provisions.

9. Links

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ES, Regulation (EU) No 910/2014 and Corrigendum
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding 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 1.1)
- General Terms and Conditions (version 1.4)
- SD Supervisory scheme for enhanced trust services as defined by the supervisor
- ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC6960)
- OCRA: OATH Challenge-Response Algorithm (RFC6287)