NFQES

BRAIN:IT

GENERAL TERMS OF TRUST, INFORMATION, CRYPTOGRAPHIC AND OTHER SERVICES

Provision and use of the trusted service of preparation and verification of certificates brainit.sk, s.r.o. with effect from 20.07.2023

Contents

Definitions and acronyms

If the general terms and conditions do not specify otherwise, the given definitions have the following meaning:

Certificate:

- Certificate or qualified certificate for electronic signature in accordance with the eIDAS Regulation;
- certificate or qualified certificate for electronic signature in accordance with the eIDAS Regulation;
- certificate for authentication of a website in accordance with the eIDAS Regulation;
- any other certificate that is used for encryption, authentication, or other purposes in accordance with the Provider's Policy, which was or is to be issued by the Provider to the Customer.

CRL - Certificate Revocation List - a list of certificates that have been revoked before their expiration date.

Trusted services - qualified trusted services for issuing and verifying certificates provided by the Provider in accordance with the eIDAS Regulation, the Law, and the Provider's Policies. Trusted services may also consist of other associated services in connection with certificates.

It is primarily about:

- certificate validation - providing information about the validity or revocation of certificates - CRL, OCSP response,
- key pair generation,
- and more...

Certificate holder - the person named in the certificate who is the holder of the private key corresponding to the public key to which the certificate is issued.

eIDAS Regulation - 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.

OCSP response - response to an OCSP request, which gives information about the validity of a certificate at a specific time.

Provider policy -

- policy of the provider of a qualified trust service for issuing and verifying qualified certificates, which applies to qualified certificates issued by the Provider in accordance with the eIDAS Regulation;
- policy of providing a qualified trust service for issuing and verifying qualified certificates, relating to other Certificates not listed in the point above.

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

Provider - brainit.sk, s. r. o., a company with its registered office at Veľký diel 3323, Žilina 010 08, Slovakia, ID number: 52577465, entered in the Commercial Register of the District Court of Žilina, Section Sro, entry number 72902/L.

Confirmation - a confirmation of the receipt of a Certificate, by which the Certificate Holder confirms, among other things, the receipt of the Certificates.

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

Party relying on the services - a natural or legal person who relies on the Trust Services of the Provider in its actions.

General Terms and Conditions or GTC - this document General Terms and Conditions for the Provision and Use of the Trust Service for Issuing and Verifying Certificates, always in their current version.

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

Contract - the Contract for the Provision of the Trust Service for Issuing Certificates concluded between the Provider and the Customer, or another contract between the Provider and the Customer, the subject of which is the provision of Trust Services.

CA Agreement - an agreement concluded between the Provider and the Certificate Holder, governing the rights and obligations of the contracting parties for the use of the Certificate.

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

Law/Act - Act No. 272/2016 Z. z. on trust services for electronic transactions in the internal market and on amending and supplementing certain acts.

1. Introduction

1.1 General information

The document General Terms and Conditions (GTC) for the Use of Qualified Trust Services Provided by the Provider brainit.sk, s.r.o. (hereinafter referred to as "General Terms and Conditions") serves to inform clients and third parties about the purpose of using the provided qualified trust services, the main rights and restrictions on their use, and the main aspects of providing qualified trust services.

The current version of the General Terms and Conditions is published on the Provider's website:

https://nfqes.sk/dokumenty/

An integral part of these General Terms and Conditions is the commitment of the participating parties to become familiar with and comply with:

- the policy of the Provider for providing qualified trust services
- the CP and CPS for qualified trust services related to the validation of electronic signatures/seals and the issuance of KC for electronic signatures/seals

1.2 Information about the provider brainit.sk and its contact details

Brainit.sk is a qualified trust service provider that carries out its activities in accordance with the requirements of Regulation (EU) No. 910/2014 and the Slovak Act on Electronic Services and Electronic Trust Services. Brainit.sk is therefore included in the trusted list of trust service providers.

The GTC regulate the basic rules for the provision and use of the Provider's Trust Services. They also regulate the rights and obligations of the Provider on the one hand, and on the other hand, they regulate the rights and obligations in the provision and use of the Trust Services of the Customer and the Certificate Holder.

These GTCs are created in accordance with the Provider's Policies.

The current effective GTCs, the Provider's Policies, and all documents and forms necessary for the provision of Trust Services are available on a medium that ensures durability, on the website of the company brainit.sk, s. r. o., and in a printed form at the individual Workplaces. They are available for inspection and familiarization for any interested party in Trust Services.

The service of issuing qualified certificates for electronic signature and seal was the subject of conformity assessment in accordance with Regulation eIDAS and the relevant ETSI standards. It is therefore a service provided at a qualified level in accordance with Regulation eIDAS.

Brainit.sk contact details:

General information:	
Company name	*brainit.sk, s. r. o.*
Company site	*Veľký diel 3323, 010 08 Žilina*
IČO	*52577465*
DIČ	*2121068763*
IČ DPH	*SK 2121068763*
Register	*Obchodný register okresného súdu Žilina, oddiel Sro, vložka číslo 72902/L*
Contact:	

Provider’s website	*https://nfqes.com*
Trust services website	*https://zone.nfqes.com*
E-mail	*info@brainit.sk*
Mobil	*+421 907 679 106*
Contact for certificate cancellation requests:	
Mobil	*+421 918 022 030*
E-mail	*info@brainit.sk*

1.3 Customer service

Brainit.sk provides qualified and non-qualified trust services through a Certification Authority (CA) and an internal Registration Authority (RA), as well as through a network of external RAs. External RAs carry out their activities to provide trust services on behalf of brainit.sk. A complete and up-to-date list of RAs and information about their contact details are available on the provider's website.

1.4 Access and provision of general conditions on a durable medium

This document presents the GTC on the basis of which contracts for the use of trusted, cryptographic, informational and other services provided by brainit.sk are concluded and forms an integral part of the contracts for the use of the relevant services.

These General Terms and Conditions (GTC) apply to all Participants, including Users, the Provider and all other Participants who have concluded a contract with brainit.sk for services provided by brainit.sk in accordance with the procedure set out in this document. These General Terms and Conditions also apply to Relying Parties who rely on electronic identification or on a trusted service provided by brainit.sk.

The GTC are publicly available on the brainit.sk website, in the brainit.sk mobile applications, and at any brainit.sk office or external RA brainit.sk. The GTC were published in Slovak.

Each Participant and each Relying Party undertakes to familiarize themselves with these GTC before concluding a contract with brainit.sk and using any of the services to which these GTC apply. By accepting these GTC, all participants, users and relying parties automatically agree to the Privacy Policy (GDPR) as well.

Depending on the way in which Participants and Relying Parties request and/or use brainit.sk services, the GTC are provided and accessible in a suitable manner in a readable form and on a durable medium as follows:

- If a participant concludes a contract with brainit.sk at the company's headquarters or at the headquarters of an external RA brainit.sk in paper form.
- When concluding a contract with brainit.sk electronically through another communication channel with brainit.sk, such as a mobile application or a personal visit to the brainit.sk headquarters or the headquarters of an external RA company of brainit.sk, the GTC will be provided to the Participant by sending an attached and electronically signed file via e-mail to the e-mail address provided by the Participant during the conclusion of the contract. If the Participant does not have an e-mail address and if the Policies and Procedures related to the specific service(s) covered by the contract allow for the provision of these services without the Participant specifying a valid e-mail address, the GTC will be sent to the Participant via a link in an SMS with instructions to immediately download and save them to their local device.

- In addition to the above, the GTC are permanently available in a readable form on the brainit.sk website in a format that allows them to be downloaded, stored, and reproduced in electronic form, as well as printed on paper. Upon request at the headquarters of brainit.sk, the GTC may be provided to Participants at any time in written form.

2. Binding of the general conditions and conclusion of the contract

These GTC are an integral part of each Contract and CA Agreement. In the event of a conflict between the general terms and conditions and the provisions in the contracts, the provision in the contracts shall prevail.

In addition to the GTC, the relevant Provider Policy, depending on the type of Certificate provided, is also binding for the provision of Trust Services by the Provider and their acquisition by the Customer.

The Provider shall inform each interested party in Trust Services about the GTC before concluding a contractual relationship with the Provider. The GTC are also permanently available in electronic form on a durable medium:

on the website https://zone.nfqes.com

in the process of requesting the issuance of a Certificate

The person interested in issuing the Certificate, who becomes the Certificate Holder, is obliged to actively express his/her own consent with these General Terms and Conditions after they have been made available, i.e. by signing the application for the issuance of the Certificate with a qualified electronic signature using his/her electronic identity card (eID) with a qualified time stamp, which informs the applicant that signing the application with a qualified electronic signature means expressing consent with the General Terms and Conditions. This qualified signature is subsequently validated, which verifies the validity of the signature, the validity and accuracy of the data, and the validity of the identification documents. Subsequently, this application for the issuance of the Certificate with a qualified electronic signature and with a qualified time stamp is kept in the RA's records. By signing and agreeing to these General Terms and Conditions, the Certificate Holder automatically agrees to the GDPR data processing principles.

Signing the application for the issuance of the Certificate with a qualified electronic signature by the applicant for the Certificates, who subsequently becomes the Certificate Holder, is a proposal for the conclusion of a contractual agreement for the provision of Trust Services addressed to the Provider, the content of which is created by these GTC.

The acceptance of the proposal for the conclusion of the contract arising from the previous paragraph by the Provider, and subsequently the conclusion of the contract between the Provider and the Certificate Holder, occurs at the moment of providing the requested Trust Service, i.e. at the moment in which the requested Certificate will be handed over to the Certificate Holder. The content of the above-mentioned contract between the Provider and the Certificate Holder is fully determined by the GTC.

After the conclusion of this contract according to the previous paragraph, the Provider shall issue a Confirmation for the Certificate Holder. The Certificate Holder is obliged to sign it with his/her qualified electronic signature.

A contract with a Customer who at that time is not a Certificate Holder shall be concluded in written form and the procedure according to the above-mentioned paragraphs shall not apply to it.

In addition to the GTC, the Provider's Policy is also binding for the provision of Trust Services by the Provider.

3. Services provided by brainit.sk

These GTC apply to the relationship between the Provider and Participants, as well as to the relationship between the Provider and Relying Parties, when providing any of the Provider's Trust Services.

3.1 Issuance of a qualified certificate for electronic signature

A qualified electronic signature certificate in accordance with Article 28 of Regulation (EU) No. 910/2014 is issued only to a natural person (Holder), or to a natural person authorized by the Holder or to a person acting on behalf of the Holder based on law or a decision of the competent authority. Depending on the profile and issuance policy, the certificate can be used to certify the authorship of electronic documents, for identification or authentication when accessing web applications, protected communication, and electronic signing of all types of documents (PDF (PaDES), XML (XaDES), TXT (CaDES), etc.). Qualified electronic signature certificates can also be used to sign document packages (ASiC-E), as well as e-mails (based on S/MIME (Secure/Multipurpose Internet Mail Extensions/Protocol for secure email transfer over the internet or cryptographic system for protecting messages transmitted via email and data stored on various media). The certificate may also contain data about the legal entity associated with the natural person in whose name the signer signs. In such a case, brainit.sk does not certify the representation of the natural person Holder towards the legal entity, but only that there is a legal relationship between the Holder and the legal entity.

The types of profiles of qualified electronic signature certificates issued by brainit.sk are described below in this chapter.

3.1.1 QC issued for a natural person for QES

The issuance of such a certificate is a qualified trust service under Regulation (EU) No. 910/2014. A qualified physical person certificate for QES is issued for the purposes of proving the authorship of a natural person in electronic documents signed electronically and to which the certificate is attached, as well as identifying the Holder with specific additional properties, as described in the certificate. All procedures and rules for its issuance and management are in line with the certification policy for providing this trust service.

3.1.2 QC issued for a natural person for AES

The issuance of such a certificate is a qualified trust service under Regulation (EU) No. 910/2014. A qualified certificate for AES is issued in compliance with all principles and procedures for the issuance of qualified certificates according to 3.1.1.

3.2 QC issued for electronic seal

A qualified certificate for an electronic seal is issued to any entity (Customer) that has the authority to act on behalf of a legal entity in accordance with the applicable national legislation. They can be used to guarantee the origin and integrity of the output data of a legal entity, such as: electronic documents, photographs, architectural projects, software, etc. This trust service of brainit.sk is provided in accordance with Article 38 of Regulation (EU) No 910/2014. The types of profiles of qualified certificates for electronic seals issued by brainit.sk are described below in this chapter.

3.2.1 QC issued for legal entity for a qualified electronic seal

The issuance of such a certificate is a qualified trust service under Regulation (EU) No 910/2014. An attribute in the certificate contains information that the certificate is qualified and shows whether the private key was used to create the electronic seal. Brainit.sk will issue the certificate and deliver it to the person authorized by the legal entity. By accepting these GTC when requesting this service, it is considered that the Holder agrees to use a qualified device to create a qualified electronic signature.

3.2.2 QC issued for legal entity for advanced electronic seal

The issuance of such a certificate is a qualified trust service under Regulation (EU) No 910/2014. A qualified certificate for AESeal is issued in compliance with all principles and procedures for the issuance of qualified certificates according to 3.2.1.

3.3 QC issued for authentication of website

A qualified certificate for website authentication is issued for the purpose of certifying a website by a specific natural or legal person. It is intended for use to create the certainty of the visitor that the website is managed by a real and identified entity. The use of SSL technology ensures reliable connectivity under a secure protocol for exchanging information between the website and its visitors. This qualified trust service is provided by brainit.sk in accordance with Article 45 of Regulation (EU) No 910/2014.

3.4 QC issued for qualified timestamp

The issuance of a Qualified Electronic Time Stamp (QEST) is a qualified trust service provided by brainit.sk in accordance with Article 42 of Regulation (EU) No 910/2014. QESTs are issued to natural persons and legal entities.

A QEST provides a high level of assurance of the accuracy of the date and time that is shown on it, as well as the integrity of the data that is submitted to brainit.sk. This data can include an electronic signature, an electronic seal, a hash of unsigned electronic documents, or a hash of other electronic content.

QESTs can be integrated into the process of creating, sending, or receiving electronic signatures/seals, electronically signed documents, and electronic transactions. They can also be used for archiving electronic data, and more. This service uses technology to bind the date and time to the data in a way that eliminates the possibility of undetected changes to the data and provides the ability to prove that an electronic document or other electronic item was signed at a given time, even after the QEST has expired.

3.4.1 Specific requirements relating to relying parties

The main obligation of the Relying Party is to check the validity of the signature/seal on the electronic time stamp token (TST). The Relying Party must check the validity of the time stamp unit (TSU) as well as the validity period of this certificate. If time stamps are checked after the validity period of the TSU certificate has expired, the Relying Party must:

- Check the certificate with the time stamp in the certificate revocation list (CRL).
- Check the usability of the used hash algorithm.

- Verify the security of the used electronic signature by checking the usable combination of asymmetric and hash algorithms.

When relying on a qualified electronic time stamp, the Relying Party is obliged to:

- Verify that the qualified electronic time stamp was correctly signed and that the private key used to sign the time stamp was not compromised until the time of verification.
- Take into account all limitations on the use of the time stamp stated in these terms and conditions and in the relevant policies and procedures.
- Take into account all other measures prescribed in these terms and conditions and in the relevant policies and procedures.

3.5 Qualified service of verification of qualified electronic signatures/seals

Qualified validation of a qualified electronic signature/seal is a qualified trust service in accordance with Article 32, 33 and 40 of Regulation (EU) No. 910/2014. This service is used to verify electronic signatures, electronic seals, registered e-mail services and certificates related to these services issued and provided by brainit.sk. Verification is also carried out through qualified certificates for website authentication. The qualified validation service is provided by brainit.sk as a qualified trust service provider and by providing it, a special document (result of the validation process) confirming the validity, or the results of the validation process, is generated and handed over to the Client.

In the process of verifying a qualified electronic signature/seal, brainit.sk confirms the validity of the qualified electronic signature/seal provided that:

- The certificate that accompanied the signature/seal at the time of signing was a qualified electronic signature/seal certificate meeting the requirements of Regulation (EU) No. 910/2014.
- The qualified certificate was valid at the time of signing.

This service can be provided to verify qualified certificates for electronic signatures, electronic seals and other qualified certificates issued by qualified trust service providers included in the trusted list of the European Commission. These trust services of brainit.sk are provided in accordance with Article 33 and Article 40 of Regulation (EU) No. 910/2014. The same rules and regulations apply to the verification of electronic signatures and electronic seals from different trust service providers as those mentioned above in this chapter.

3.5.1 Purpose and limitations of service use

The purpose of the service is to provide a qualified trust service for the validation of qualified electronic signatures and seals. The expected way to use the service is to integrate it into the processes of the Applicant for the verification of the validity of electronically signed documents or directly by the end user using the NFQES portal.

The service is provided in accordance with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). The Act No. 272/2016 Z. z. on trust services for electronic transactions in the internal market and on amending and supplementing certain laws (the Act on trust services) and the Scheme for the Supervision of Qualified Trust Services defined by the supervisory authority - NBÚ SR No. 05968/2019/ORD-001.

The operation of the qualified trust service is governed by the general requirements for the provision of qualified trust services in accordance with ETSI EN 319 401 "Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers".

The service can be used exclusively for proper and legal purposes and in accordance with applicable laws and regulations and the Provider's regulations for purposes within the processes of the End User.

The service can be used through pre-defined interfaces after the service is made available by the Operator and exclusively for the defined purpose.

3.6 Qualified electronic mailbox service

Qualified registered electronic mailbox service is a trust service that enables electronic transmission of data between third parties and provides evidence of the identity of the sender and recipient of the transmitted data, the time of sending and receipt of the data, and protects the transmitted data from the risk of loss, theft, damage, or unauthorized changes. The service provides:

- high level of trust with regard to the identification of the sender
- identification of the sender before the delivery of the data
- secure sending and receiving of data through a qualified electronic signature or a qualified electronic seal of brainit.sk in a way that excludes all possibilities of undetected changes in the data
- any change in the data necessary for the purposes of sending or receiving the data is clearly marked for the sender and for the recipient of the data
- the date and time of sending and receiving, as well as any change in the data, is marked with a qualified electronic time stamp

When providing this service, brainit.sk signs with an electronic seal and gives the sender proof (electronic delivery) of the facts of sending, receipt and integrity of the transmitted content.

This trust service of brainit.sk is provided in accordance with Article 44 of Regulation (EU) 910/2014. Proof of sent messages can be stored for a period of 10 years in the Provider's storage. It can be provided to contracting parties in accordance with the applicable prices and conditions. Types of electronic recommended delivery services provided by brainit.sk

3.6.1 Specific requirements for the provision of a qualified electronic registered delivery service

Successful delivery of electronic content

- The content is considered successfully delivered if the content sent by the sender has left the sender's information system and is no longer under the sender's control.
- The shipment is considered delivered if the content sent by the sender has successfully entered the recipient's information system.
- When using the web portal, the successful sending is considered to be the receipt of the electronic message from the web browser of the Participant using the portal on the backend (server) of brainit.sk and the successful delivery is considered to be the receipt of the sent message in the virtual mailbox accessible in the recipient's account through the web portal.
- When using the qualified REM service, the successful sending is considered to be the time of receipt of the electronic message into the information system on the brainit.sk email server

(backend) and the receipt is considered to be the receipt into the electronic mailbox served by brainit.sk on the brainit.sk email server.

Brainit.sk ensures that the service protects the transmitted electronic content from loss, theft, disruption of integrity or unauthorized change and meets the requirements of Regulation (EU) No. 910/2014.

3.7 Electronic signature and seal storage service

The service of storing electronic signatures and seals is provided by brainit.sk in accordance with Article 34 and Article 40 of Regulation (EU) No. 910/2014. These trust services ensure the safe and reliable long-term storage of all types of electronic signatures and seals attached to documents (without storing the documents themselves in the repository) and/or electronically signed/sealed documents (with storage) of Participants and provides evidence of the storage process with the ability to long-term verify electronic signatures/seals.

Data objects, relevant evidence of storage and additional information necessary for their verification are accessible through the service interface or by submitting a specific request for the provision of data and/or evidence. They can be provided separately or in an I/O (input/output) package that is securely protected by encryption. In any case, they will be delivered only to the Participant or its authorized representative. Brainit.sk keeps information about all prepared I/O packages, including the date of the event and the criteria according to which the stored objects included in the package were selected.

The request must include the person requesting the data, the reasons for requesting it, and how they want to receive it, such as by email or on an electronic medium. Brainit.sk reserves the right to approve or reject the execution of the request without having to justify its rejection, or to inform the applicant about it, except in cases specified in the legislative act. For the purpose of providing data and evidence, brainit.sk may charge fees to ensure the execution of the submitted request. Brainit.sk does not use any external organizations supporting the storage service. After the data retention period has expired, the data will be deleted.

4. Price for reliable services and payment terms

The current prices for issuing Certificates are listed in our price list published on the website https://nfqes.com (hereinafter referred to as the "Price List"). The price for providing a Trust Service is determined in accordance with the Price List that is valid during the provision of the Trust Service, unless otherwise agreed between the contracting parties.

Prices for issuing Certificates may be individually agreed with the Customer directly in the contract, confirmed order or also in another document.

The value of the price for Trust Services is to be paid by the Customer by wire transfer based on an invoice issued by the Provider after providing the requested Trust Service. The payment term for this invoice is 2 weeks, i.e. 14 days, unless otherwise provided by generally binding legal regulations or the given contract. The price for these Trust Services is paid on the day on which this amount is credited to the Provider's bank account in full.

It is necessary for the invoice issued by the Provider to contain all the requirements of a tax document listed in Section 74 (1) of Act No. 222/2004 Coll. on value added tax as amended. The Customer has the right to object to the content or formal defects of the invoice to the Provider during the validity of its payment term. The Provider will assess the Customer's objections and, if they are justified, will subsequently issue a new invoice, the payment term of which will then begin to run from the day on which it was delivered to the Customer.

If the Customer does not pay the entire amount for the provided Trust Services within the payment term according to the VP or the given contract, the Provider of the Trust Service has the right to immediately withdraw from the contract, which also results in the cancellation of each Certificate for which he did not receive payment.

5. Issuance of certificates

Certificates under the mentioned GTC are issued exclusively to the HSM Device, remotely mediated by the Application, only based on a request from the applicant for Certificates. If the conditions set by these VPs and the Provider's Policy are met, the Provider is obliged to issue the Certificate to the Holder and deliver it in the immediate future. The Provider also issues a Confirmation to the issued Certificates, which is signed by the Certificate Holder. The Confirmation specifies the specific Certificate that was issued for the Certificate Holder. The Trust Service is provided at the time of the issuance of the issued Certificate by the Certificate Holder.

5.1 Restrictions on the use of the services provided

The Participant undertakes to take all necessary measures to minimize and limit the damage resulting from the use of services that exceed the limitations of their use set out in these VPs. Relying parties agree and undertake to take all necessary measures when relying on the electronic identification service or trust service provided by brainit.sk to monitor and comply with the limitations on the use of services as set out in these GTC.

5.1.1 Time limits

Each certificate issued by brainit.sk can only be used until its validity expires. The validity period of the certificates is stated in them. If the certificate has been revoked, the signer/creator must not use the private key to create an electronic signature/seal.

5.1.2 Designated purpose

Certificates issued by brainit.sk will be used in accordance with their intended purpose, as described in these GTC, in the relevant policies and procedures of brainit.sk and in the relevant law. Verification of the intended purpose of the certificate will be carried out on the basis of the data stated in the certificate profile:

- policy/practice in accordance with which the electronic signature/seal certificate is issued and managed
- intended purpose and limitations of the effect of the certificate with regard to the purposes for which it is used
- details of the signer/creator of the certificate

6. Restrictions on the use of certificates

Each certificate issued by the Provider can be used in the usual way, only for the purpose for which it is intended, in accordance with the terms and limitations set out in the relevant Provider Policy. The certificate is intended exclusively for the creation of an electronic signature or advanced electronic signature of the certificate holder. Since the Device is a qualified device in accordance with the eIDAS Regulation, it is possible to create a qualified electronic signature using the Certificate.

The validity period of the Certificates is limited. After the validity period or revocation of the Certificate, it is forbidden to use the Certificate, even for the purpose for which it is intended. The result of using a Certificate that is invalid or has been revoked, which is also intended for creating an electronic signature, will subsequently be invalid.

The verifiability of the electronic signature has limitations, i.e. after the validity period of the Certificate based on which they were created, it is not guaranteed that it will be possible to verify the validity of the said electronic signature retroactively. To ensure the long-term verifiability of this electronic signature even after its validity has expired, it is necessary to use specialized services for this purpose in a reasonable manner, even during the validity of the Certificate, for example, the service for storing electronic signatures and/or the service for electronic time stamping.

The use of the Certificate to create an electronic signature does not yet guarantee that the created electronic signature can be used for the planned purpose. It also does not mean that they will be in the required format acceptable to third parties. The format of the electronic signature is determined by the application used to create the electronic signature.

If the Customer or the Certificate Holder uses the Certificate in a way that violates the rules set out in these VPs or relies on the Certificate in violation of these limitations and he or a third party suffers damage because of this act, the Provider is not liable for it in accordance with Article 13(2) of the eIDAS Regulation.

7. Specific conditions for issuing qualified trust services

7.1 Acceptance of the certificate

After receiving a qualified certificate, the Participant is obliged to verify its content for the correctness of the data and the existence of the public key corresponding to the private key that he owns.

If the certificate contains incorrect data, the certificate will be immediately revoked. If the Participant objects that the issued qualified certificate contains errors or defects within 3 (three) days of its publication in the certificate repository, brainit.sk will remove it free of charge by issuing a new certificate, unless they occur as a result of providing incorrect data. If no objections were raised, the content of the certificate is accepted. The rules set out in this point apply to the issuance of the certificate as well as to the renewal of the certificate.

A qualified certificate is accepted by the Participant if one of the following conditions is met:

- Express approval/confirmation by the Participant
- The Participant used the qualified certificate for the first time
- After 3 (three) days from the date of issuance of the qualified certificate, if the Participant does not raise an objection to the content of the certificate within the specified period

In the case of electronic signature certificates, respectively electronic seal certificates, the obligation according to the above, the possibility of objection, as well as the assumptions under which the certificate is considered to be accepted, always apply only in relation to the Signatory, respectively the Creator, regardless of whether the actual issuance of the certificate is paid by him or by a third party (another Participant) who also entered into a contractual relationship with brainit.sk under these GTC.

8. Rights and obligations of the customer and certificate holder

Both the Customer and the Certificate Holder are obliged to comply with these VPs and generally binding legal regulations of the Slovak Republic. The Customer is entitled to use the Trust Services provided by the Provider in accordance with the contract, these VPs and the Provider's Policies. The Customer has the right to request the revocation of the issued Certificate regardless of the consent of the Certificate Holder.

If the Customer is a consumer, he/she has the rights in the event of defects in the Trust Service in accordance with § 622 and § 623 of the Civil Code.

In particular, the customer is obligated to:

a) Provide the Provider with all data and documents required by the Provider's Policies for the provision of the requested Trust Service. The data and documents must be true, current, and complete.
b) In the case of providing data that are necessary for the provision of the Trust Service, ensure in advance that these data are sent to the Provider in a way that guarantees their confidentiality and integrity (for example, sending an encrypted file electronically and sending a password through a separate channel).
c) Use the Certificate and the generated key pair only for the purposes for which they are intended, in accordance with the applicable laws and restrictions on their use set out in the VPs.
d) Exercise due care in using the Certificate and in relying on the Certificate, in accordance with Part 10 of the VPs.
e) Refrain from unauthorized use of the private key of the Certificate Holder if the Customer and the Certificate Holder are not the same person.
f) In cases where the Customer generates cryptographic keys for which the Certificate is to be issued, the Customer is required to create a key pair of the prescribed length, using the algorithm required by the Provider's Policy relating to the requested Certificate.
g) Allow the private key for which the Certificate is issued to be used for cryptographic functions exclusively within the Device and under the exclusive control of the Certificate Holder.
h) Provide the Provider with immediate and prompt cooperation, if requested, in verifying the data required for the issuance of the Certificate.
i) During the validity of the Certificate, immediately notify the Provider of any changes, errors, or inaccuracies in the data that are stated in the Certificate.
j) During the validity of the Certificate, immediately notify the Provider if there is any misuse, theft, loss, damage, destruction, compromise, or any unauthorized access to the corresponding private key or access codes (password and token) or if the Customer suspects that any of the aforementioned events may have occurred; and ensure that the Certificate Holder refrains from using the private key and Certificate whose validity period has already expired, has been revoked, or has been compromised (including the case that the Provider itself has been compromised and the Customer is aware of it).

The Certificate Holder has the right to use the Certificate issued to him by the Provider in accordance with the contract and these GCT.

The holder of the certificate is obligated to:

k) Immediately after obtaining the Certificate, check the correctness and timeliness of the data stated therein and always provide only up-to-date, accurate and current data and documents in connection with the Trust Services;

l) Exercise due care when using the Certificate and relying on the Certificate, in accordance with Part 10 of these VPs;

m) Use the Certificate and the generated key pair only for the purposes for which they are intended, in accordance with applicable laws and restrictions on their use set out in the VPs;

n) Protect the access code (password and token) from unauthorized access, as well as against loss, compromise, destruction, or misuse;

o) During the validity of the Certificate, immediately notify the Provider of any changes, inaccuracies, or inaccuracies in the data stated in the Certificate;

p) During the validity of the Certificate, immediately notify the Provider if there is any misuse, theft, loss, destruction, compromise, or any unauthorized access to the corresponding private key, access codes (PIN), recovery code (PUK), or to the device on which the keys are stored or if the Certificate Holder suspects that any of the aforementioned events may have occurred and refrain from using the private key and Certificate whose validity period has already expired, has been revoked, or has been compromised (including the case that the Provider itself has been compromised and the Certificate Holder is aware of it).

The Customer or the Certificate Holder requests the Provider to revoke the Certificate using the contact details specified in Article 3 of the GTC.

9. Rights and obligations of the provider

The Provider is entitled to refuse to provide the Trust Service, or to restrict the scope of its provision to the client (for example, by not including all the required attributes in the Certificate) if the conditions for issuing Certificates defined in the Provider's Policy or these GTC have not been met.

The Provider is entitled to revoke the Certificate in the cases specified in the relevant Provider's Policy, mainly if:

- The Provider notices that the conditions for issuing the Certificate were not met in accordance with the eIDAS Regulation, the Act, or the Provider's Policy;
- The Provider notices that the Device on which the keys are stored or its software components may be compromised;
- The Court orders the Provider to revoke the Certificate;
- The Customer has not paid the agreed price of the Trust Services within the predetermined period, even after a reminder sent electronically by the Provider;
- The Customer does not publish the contract with the Provider within three months of its conclusion in cases where it is a contract that must be published in accordance with Section 5a of Act No. 211/2000 Coll. on the Freedom of Access to Information and on Amendments and Supplements to Certain Acts (Act on Freedom of Information);
- The contract with the Customer or the Certificate Holder is terminated or expires or if the Certificate Holder does not sign the Confirmation;
- The Customer or the Certificate Holder breaches the obligations set out in these General Conditions, the contract, or generally applicable laws and regulations;

- The Provider learns of any changes that affect the validity of the Certificate, especially in cases where the data stated in the Certificate are false or outdated or the Provider learns of the theft, loss, or compromise of access codes, etc.;
- The Provider finds out that the Customer or the Certificate Holder has died (if it is a natural person) or has ceased to exist (if it is a legal person);
- The Customer or the Certificate Holder requests revocation;
- The Certificate is no longer in accordance with the Policy within which it was issued;
- The cryptography used for the Certificate no longer ensures the connection between the Certificate Holder and the public key.

The Provider is entitled to publish the name of the Customer on its website as a reference if the contract does not specify otherwise.

The Provider is obliged to provide Trust Services in accordance with the eIDAS Regulation, the Act, and its own Policies in force at the time of their provision.

10. Information for parties relying on trust services

Relying parties are solely responsible for deciding whether to trust and rely on a Certificate issued by the Provider and the information contained therein. In the event of a decision to trust the Provider's Certificates, it is the responsibility of the relying parties to comply with the obligations described in this 10th part of the VP, otherwise they are solely responsible for the legal consequences thereof.

The relying party is aware that the validity of Certificates, CRLs, and OCSP responses issued by the Provider is limited in time:

- A Certificate is valid for the period of validity specified in the body of the Certificate or until the moment of its revocation before the expiry of the validity period;
- A CRL is valid for the period of validity specified in the body of the CRL, and to obtain the most accurate information about revoked Certificates, it is always necessary to start from the most recent CRL, i.e. the one that the Provider published last;
- An OCSP response is valid at the time specified in the body of the OCSP response by the "producedAt" item. The ProducedAt item is only the time of signing the OCSP response and has nothing to do with the validity of the certificate.
- Only those CRLs and OCSP responses can be used to validate signatures or seals where the thisUpdate item contains the time and date after the time and date of signature, which is within the validity period of the certificate and is considered to be the time at which the validity of the certificate is being verified.

For reliance on any Certificate issued by the Provider, the relying party is required to exercise reasonable care, especially it is its obligation to:

- Assess whether the use of the Certificate is in accordance with its intended purpose and whether it is suitable for that purpose;
- Check whether the use of the Certificate is not in conflict with the restrictions on the use of the Certificate set out in the Certificate itself, these General Conditions, or the Provider's Policies that apply to the Certificate;
- Use only designated and suitable hardware or software when working with the Certificate, including its validation;

- Verify the validity of the relevant Certificate by using an application that validates a qualified certificate using a trusted list published by the NBÚ and a suitable CRL or OCSP response with the thisUpdate item containing the time and date after the time of signature or seal.
- Implement any other verifications that may be required for a specific type of Certificate or its use in accordance with the Provider's Policies or standards;
- Verify the other certificates in the certification path up to the so-called "trust anchor" in the same way as in points a) - e). The trust anchor is stored in the trusted list published by the NBÚ. Certificates stored in the trusted list represent the "Trust anchor".

The relying party also takes note that the Provider archives information related to issued Certificates for the purpose of providing evidence for a certain period in accordance with Article 12 of the GTC.

For reliance on a CRL or OCSP response issued by the Provider, it is the responsibility of the relying party to exercise reasonable care. The obliged party is particularly required to verify that the certificate with which the CRL or OCSP response was signed belongs to the Provider using a trusted list issued by the NBÚ and at the same time to proceed analogously in accordance with Article 10 of these GTC.

11. Provider's liability, warranty, and their limitaitons

The Provider is only liable for damage caused by non-compliance with its obligations under the eIDAS Regulation in accordance with Article 13 of the eIDAS Regulation.

The Provider is obliged to provide Trust Services in accordance with generally applicable laws and the Provider's Policies. The Provider is liable for defects in the provided Trust Service in accordance with generally applicable laws.

The Provider is not liable for indirect losses or damages that have occurred to the Customer, Certificate Holder, Relying Party, or a third party in connection with the use of Trust Services.

The Provider is not liable for damage (including lost profits) that has occurred to the Customer, Certificate Holder, Relying Party, or any third parties due to:

- Breach of obligations by the Customer, Certificate Holder, or Relying Party set out in generally applicable laws, these VPs, the relevant contract, or the Provider's Policies, including the obligation to exercise reasonable care when using the Certificate and relying on the Certificate;
- Failure to provide necessary cooperation by the Customer or Certificate Holder;
- Technical properties, configuration, incompatibility, inappropriateness, or other defects in the software or hardware used by them;
- Use of, or reliance on, a Certificate whose validity has expired or has been revoked;
- The Certificate was used in violation of its intended purpose or restrictions set out in the Certificate, in these VPs, or in the Provider's Policies;
- Delay or non-delivery of requests for verification of the status of the Certificate to the Provider, for reasons that are not on the Provider's side (especially cases of unavailability or congestion of the internet network, or defects in the device or technical equipment used by the verifier);
- Failure to provide one of the Trust Services or its unavailability during planned maintenance or reorganization announced on the Provider's website;
- Force majeure

The Provider is not liable for damage that has occurred to the Relying Party due to the fact that the Relying Party did not comply with Article 10 of these VPs when relying on the Provider's Trust Services or on the electronic signature or seal made on their basis.

The Provider is also not liable:

- For the fact that an unauthorized person gained access to the Customer's or Certificate Holder's access codes;
- For damage caused using the Certificate if the Customer or Certificate Holder does not act in accordance with its obligations, mainly if an unauthorized person gains access to the access codes and the Customer or Certificate Holder does not request the Provider to revoke the Certificate or if the Customer or Certificate Holder does not notify the Provider of changes in the data.

The Customer and Certificate Holder use Trust Services at their own risk and bear all costs for telecommunications or other technical means necessary for the use of the Provider's Trust Services (for example, for software necessary for the creation of an electronic signature or seal based on the Certificate).

12. Protection of privacy and personal data

12.1 Processing of personal data

Brainit.sk conducts its activities of providing trustworthy services in accordance with the requirements of Regulation (EU) 2016/679 (GDPR), applicable law, and in accordance with its valid Privacy Principles, which constitute an integral part of these GTC and the contract with the Participant.

The valid privacy principles of the company Brainit.sk include:

- Privacy principles applicable to trustworthy, informational, cryptographic, and other services provided by Brainit.sk (all services).
- Additional privacy principles that Brainit.sk may adopt and apply in connection with the provision of certain services.

The privacy principles applicable to trustworthy, informational, cryptographic, and other services provided by Brainit.sk relate to activities performed in the provision of services under these General Terms and Conditions. In connection with some of its services, Brainit.sk may additionally establish and implement specific privacy principles concerning the processing of personal data by Brainit.sk in the provision of these services. In case of a conflict between the privacy principles related to trustworthy, informational, cryptographic, and other services provided by Brainit.sk and these specific principles, the specific principles take precedence but only concerning the processing activities related to the provision of the respective services to which these policies apply. In case of gaps in the specific principles, the provisions of the privacy principles applicable to trustworthy, informational, cryptographic, and other services provided by Brainit.sk apply.

Before entering a contract, the Participant familiarizes themselves with the Privacy Principles that apply to the services requested by the Participant. This allows them to understand how Brainit.sk processes personal data, the types of personal data processed, and the purposes for which it is processed. The Participant is also informed about their rights and other important issues related to the protection of personal data in accordance with GDPR.

The provision of services is inherently linked to the acceptance, transmission, storage, and processing of the Participant's data through Brainit.sk systems, relying parties, as well as the exchange of such data between them and the provider in accordance with applicable legislation and the contractual relationships formed among all the parties. The Participant is familiar with the above and agrees that their data may be provided to third parties for the purpose of service provision.

The Provider processes personal data of data subjects in accordance with relevant legal regulations. The Provider can disclose this data to third parties if required by applicable laws or regulations.

For informing the data subjects or individuals interested in Trusted Services about the processing of personal data carried out by the Provider in the provision of Trusted Services, the Information on the Processing of Personal Data serves:

- Always available in electronic form online at https://nfqes.com
- About which the Certificate Holder is informed during the process of applying for the issuance of the Certificate.

The Provider records and archives all essential information and documents related to the issuance or revocation of the Certificate, including the personal data of the Customer, Certificate Holder, and any persons authorized to act on their behalf or authorized by them, for a period of 10 years from the date of revocation or expiration of the relevant Certificate.

The Certificate Holder acknowledges that if an electronically signed document is signed based on the Certificate, the recipient of this electronic document, or any individuals with access or future access to this electronic document, will have access to their personal data stated in the Certificate.

13. Resolution of disputes and complaints

The user is entitled to send a complaint, suggestion, or claim to the Provider of the Trusted Service by email at ca@nfqes.sk. The Provider will respond within 30 days of receiving it; in the case of more complex complaints or claims, the Provider reserves the right to extend this period.

The courts of the Slovak Republic have exclusive jurisdiction to settle any disputes between the Provider and the Customer or Certificate Holder. If the Customer or Certificate Holder is a consumer, they are entitled to contact an out-of-court dispute resolution entity, such as the Slovak Trade Inspection or another legal entity registered in the list according to § 5 para. 2 of Act No. 391/2015 Coll. on alternative dispute resolution for consumer disputes, as amended. Before resorting to judicial or extrajudicial dispute resolution, it is the obligation of the contracting parties to attempt to resolve the dispute by mutual agreement in advance.

14. Governing law

The legal relationships between the Provider and the Customer or Certificate Holder are governed by the legal regulations of the Slovak Republic.

Legal relationships not expressly regulated by these General Terms and Conditions, or the contract shall be governed by the relevant provisions of Act No. 513/1991 Coll., the Commercial Code, as amended, and other generally binding legal regulations. If the Customer or Certificate Holder is a consumer, the legal relationships between them and the Provider, which are not expressly regulated by these General Terms and Conditions, shall be governed by the provisions of Act No. 40/1964 Coll., the Civil Code, as amended.

15. Duration and termination of contracts

The contract between the Provider and the Customer is concluded for an indefinite period, unless otherwise stated. The contract between the Provider and the Certificate Holder is always concluded for a fixed period, until the expiry of the validity or the cancellation of the Certificate to which the contract relates.

The contract between the Provider and the Customer may be terminated:

a) by mutual agreement of the parties at any time;
b) by termination by either party if the contract is for an indefinite period; The notice period is 2 months and begins to run from the first day of the calendar month following the month in which the written notice was delivered to the other party;
c) termination by either party in the event of a material breach of the contractual obligations by the other party.

The following are considered to be a material breach of the contractual obligations, which gives rise to the right to terminate the contract:

a) if the Customer fails to pay the full price for the trusted services provided in the agreed time period;
b) if the Certificate Holder or the Customer uses the Certificate in a way that is in violation of the law, these GTC, or the Provider's Policies;
c) if the Customer or the Certificate Holder fails to request the cancellation of the Certificate in cases specified in these GTC or the contract;
d) other reasons in accordance with the generally applicable laws of the Slovak Republic.

If the Provider exercises its right to terminate the contract, it also has the right to revoke the Certificate that is the subject of the breach of obligation by the Customer or the Certificate Holder.

In the event of the termination of the contract, the Customer's obligation to settle any debts that have arisen in connection with the use of the Trusted Services does not cease.

The termination of the contract between the Provider and the Customer, or the Certificate Holder, does not affect those provisions from which it follows by their nature that they should continue to exist after their termination.

15.1 Contract, conclusion, subject of contract

Brainit.sk will provide, either free of charge or for a fee, services to which these Terms and Conditions apply, subject to and with strict compliance by the participant/signatory/creator of the contract concluded in accordance with these GTC, as well as in accordance with the applicable law. Services are diverse, constantly supplemented and modified to improve and expand them, and on this basis, brainit.sk may unilaterally change their number, properties, and conditions of their provision at any time within the limits of the applicable legislation.

Services of brainit.sk can be requested, or provided, in various ways depending on their nature and in accordance with these Terms and Conditions. Requesting a service and concluding a contract requires the secure identification of the Participant in accordance with the level of security required for the specific service and the consent of the Participant to these Terms and Conditions. Before requesting a service, the Participant will become familiar with all the Policies and procedures applicable to the relevant service. By requesting a service, the Participant accepts these Terms and Conditions.

Different services of brainit.sk can be requested in different ways and not every way of requesting provides the opportunity to request each of the services. Brainit.sk maintains up-to-date information on the ways to request and use different types of services on its website.

Services of brainit.sk can be requested in any of the following ways:

15.1.1 By a personal visit to the head office of brainit.sk

The procedure for requesting a trusted service at the headquarters of brainit.sk requires the physical presence of the Participant in cases where the Participant is a natural person, or the presence of a legal representative or authorized representative duly authorized by a notarized power of attorney, if the Participant is a legal entity.

For a natural person:

For the unambiguous identification and verification of the identity of the Participant, the Participant shall provide the following information:

- full name (as in the identity document),
- identity document (national ID card, international passport, or other identity document),
- national identification number, if applicable,
- contact information – mobile phone number, email address and permanent address.

After the successful verification of the identity of the Participant, the authorized operator from the internal Registration Authority of brainit.sk:

- proposes a contract on qualified trusted services signed in the name of brainit.sk and keeps all submitted documents relating to the contract. The contract will be signed by the Participant in paper form together with these Terms and Conditions, the applicable Privacy Policy of brainit.sk and all other documents relevant to the requested service.
- confirms the request for issuance and sends an electronic request for issuance of the certificate to the operational certification authority of brainit.sk.
- records the issued certificate on the device for creating a secure signature and delivers it to the signer or authorized person (if appropriate).

The conclusion of a contractual relationship with a natural person arises:

- based on a request for the issuance of a certificate that refers to these GTC,
- based on the signature of the contract in paper or digital form (qualified e-signature).

For a legal entity:

The identification of a legal entity is performed by the Registration Authority (RA) by checking the relevant registers based on the provided registration or other unique identification number of the legal entity (LE). The identification of the LE and the verification of the authorized representative are carried out on-site based on the information provided by the Participant through documents sent remotely or by personal meeting. Such identification verifies all the data that will be included in the issued certificate, as well as the authorization of the legal representative of the person who attended the physical meeting at the headquarters of brainit.sk.

In the case of a legal entity, the following documents must be submitted:

- decision of the court or other document certifying the establishment of the legal entity,
- document confirming the integrity,
- unique national identifier,
- other relevant documents.

After copying all the required documents with the consent of the person who submitted the request, the copies remain in the brainit.sk records. For the avoidance of doubt, such consent does not constitute consent under Regulation (EU) No 679/2016, but contractual consent and is a mandatory condition for the conclusion of the contract. Verification of the data contained in the submitted documents is carried out by verifying the "true copy or original" and a handwritten signature signed by the person representing the Participant in front of the RA employee.

The certification of the identity of the legal entity has two purposes: (1) verifying whether the legal entity exists or not at the time of the review of the request, and (2) verifying whether the person acting on behalf of the legal entity has the necessary authority to request the relevant trusted services and validly conclude a contract for their provision on behalf of the Participant according to these GTC.

The conclusion of a contractual relationship with a legal entity arises:

- Based on the signature of the contract in paper or digital form (qualified e-signature),
- By a binding order for the supply of services.

15.1.2 By personally visiting the external Registration Authority brainit.sk

The process of requesting a service and entering a contract begins with a personal meeting of the individual Participant or their legal representative or duly authorized representative of the legal entity Participant at the workplace of the external Registration Authority and the submission of a request to the Registration Authority for the respective service. The request can be submitted to the external registration authority of Brainit.sk for any of the services provided by Brainit.sk, in connection with which the respective external registration authority is authorized to act as the registration authority of Brainit.sk. After the Participant's request is submitted to the registration authority, the same procedure for requesting the service will be followed, as mentioned above in this section.

16. Final provisions

The Provider is entitled to unilaterally modify the General Terms and Conditions or the Price List for reasons related to the commercial policy of providing Trusted Services, changes in generally applicable legal regulations, changes in standards regulating the provision of Trusted Services, due to technical, security, or organizational changes in the systems used to provide Trusted Services on the part of the Provider, as well as for the purpose of improving the quality, security, or availability of Trusted Services. In such a case, the Provider is obliged to notify the Customer and Certificate Holders of the changes at least 30 days before the effectiveness of these changes, by sending an informational electronic message to the provided email address in advance and by also publishing them on the Provider's website. If the Customer or Certificate Holder disagrees with the change to the binding document, they have the right to terminate the contract with the Provider within 30 days from the date of sending this information to the Provider, with immediate effect. The notice can be sent to the Provider's registered office address or to the email address info@nfqes.sk. If the Customer or Certificate Holder does not reject the proposed change in writing by the effective date of the change, it is deemed that they agree with it, and this change becomes binding for them from the date of its effectiveness.

For the delivery of legal acts and other legal documents between the Provider on one side and the Customer or Certificate Holder on the other side, the contact details provided by the parties to each other are used, especially the email address and the residential/registered office address. It is the contractual party's obligation to promptly notify the other contractual party of any changes to their contact details. Until the notification of the change of contact details to the other contractual party, the provided contact details are considered accurate.

If any provision or part of these General Terms and Conditions or the contract is or becomes invalid or ineffective, the validity and effectiveness of any other provision or remaining part of the respective provision are not affected by it. The parties undertake to replace such invalid or ineffective provision with a provision on which they would agree if they were aware of such invalidity or ineffectiveness.

If any provision, part, or part of these General Terms and Conditions is or becomes invalid, ineffective, or unenforceable, the remaining part of the relevant provision or the remaining part of the General Terms and Conditions is not affected by it.

These General Terms and Conditions are valid and effective from 20.7.2023.

This document is published on the brainit.sk website in Slovak. In case of any discrepancies, the Slovak text takes precedence.