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

Content

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;
- website verification certificate in accordance with the eIDAS regulation;
- any other certificate that serves for encryption, authentication or other purposes in accordance with the Policy of the Provider, which the Provider was or is to issue to the Customer.

CRL – Certificate Revocation List - list of certificates revoked before the expiration date.

Trusted services - qualified trusted services for the preparation and verification of Certificates provided by the Provider in accordance with the eIDAS Regulation, the Law, and the Provider's Principles. Trusted Services may also consist of other associated services in connection with the Certificates.

It is primarily about:

- verification of Certificates – provision of information on the validity or cancellation of Certificates – CRL, OCSP response,
- generation of key pairs,
- and others...

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

eIDAS regulation - Regulation of the European Parliament and the Council of the EU No. 910/2014 of 23.7.2014 on electronic identification and managed services for electronic transactions in the internal market and on the repeal of 1999/ES.

OCSP response - response to the OCSP request, which provides information about the validity of the Certificate at the specified time.

Provider Policy -

- the policy of the provider of the trusted service of preparation and verification of qualified certificates, which applies to qualified certificates issued by the Provider in accordance with the eIDAS regulation;
- the policy of providing a reliable service in the preparation and verification of qualified certificates, applicable to other Certificates not mentioned 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 - the company brainit.sk, p. r. about. with registered office Veľký diel 3323, Žilina 010 08, ID number: 52577465, registered in the commercial register of the District Court of Žilina, section Sro, insert number 72902/L.

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

Workplace - place where Certificates are issued. This is a place operated by the Provider - its headquarters.

Relying parties - a natural or legal person who relies on the Trustworthy Services of the Provider in their actions.

General conditions - this document General conditions of provision and use of the service creation and verification of a trusted certificate always in their effective wording.

Qualified device – a device for creating an electronic signature / seal that meets the requirements listed in Annex II of the eIDAS regulation.

Contract - Contract for the provision of the service of issuing trusted 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 Trusted Services.

Contract/Agreement with CA - an agreement concluded between the Provider and the Holder of the certificate, regulating the rights and obligations of the contracting parties when using the Certificate.

Customer - is understood as a natural or legal person to whom the Provider provides Trusted Services based on the agreed Agreement and the person who pays for these services.

Act - Act No. 272/2016 Coll. on trusted services for electronic transactions in the internal market and on the amendment of certain laws.

1. Introduction

1.1 General information

Document General conditions of use of qualified trusted services provided by the Provider brainit.sk, s.r.o. (hereinafter referred to as "General Terms" or “GTC”) serves to inform clients and third parties about the purpose of using the provided qualified trust services, the main rights and restrictions in their use and the main aspects of the provision of qualified trust services.

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

https://nfqes.com/documents/

An integral part of these general terms and conditions is the obligation of the participating parties to familiarize themselves with and comply with:

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

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

The company Brainit.sk is a qualified provider of trusted services that performs its activities in accordance with the requirements of Regulation (EU) No. 910/2014 and the Slovak Act on electronic services and electronic trusted services. As such, Brainit.sk is included in the trusted list of trusted service providers.

The general terms and conditions (hereinafter referred to as the general terms and conditions) govern the basic rules for the provision and use of the Provider's Trusted Services. And they also regulate the rights and obligations of the Provider on the one hand and, on the other hand, regulate the rights and obligations in the provision and use of Trusted Services of the Customer and the Certificate Holder.

These VPs are created in accordance with the Provider's Principles.

The currently valid General Terms and Conditions, the Provider's Policy and all documents and forms necessary for the provision of Trusted Services are permanently available on the company's website brainit.sk and in a printed version at individual Workplaces. They are available for viewing and inspection by anyone interested in trusted services.

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

Brainit.sk contact details:

General informations:	
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 request:	
Mobil	*+421 918 022 030*
E-mail	*info@brainit.sk*

1.3 Customer service

Brainit.sk provides qualified and unqualified trusted services through the Certification Authority (CA) and internal Registration Authority (RA), as well as through a network of external RAs. External RAs perform their activities to provide reliable services on behalf of brainit.sk. A complete and up-to-date list of RAs and their contact details is available on the provider's website.

1.4 Access and provision of general conditions on a durable medium

This document represents the General Terms and Conditions 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 contracts for the use of relevant services.

These GTC apply in relation to all Participants, namely in relation to Users, Providers and all other Participants who have concluded a contract with brainit.sk for services provided by brainit.sk using the procedure specified in this document. These GTC also apply to Relying Persons who rely on electronic identification or the trusted service of brainit.sk

VPs are publicly available on the brainit.sk website, in the brainit.sk mobile applications and in any brainit.sk headquarters or external RA brainit.sk. VP was published in Slovak.

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

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

- When concluding a contract with brainit.sk at the company headquarters or at the headquarters of the external RA brainit.sk in paper form.
- When concluding a contract with the brainit.sk company electronically, through another communication channel with the brainit.sk company such as a mobile application or by personally appearing at the brainit.sk head office or at the head office of the brainit external RA. sk company, the VP is provided to the Participant by sending it as an attachment and an electronically signed file by e-mail to the e-mail address that the Participant provided when concluding the contract. If the Participant does not have an e-mail address and if the Policies and procedures regarding the specific service(s) that are the subject of the contract do not allow the provision of these services without providing the Participant with a valid e-mail

address, the GTC are sent to the Participant via a link in an SMS with instructions to the Participant immediately downloaded and saved them to his local device.

- In addition to the above, VPs are available for a long time 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. The Participant's VP can be provided in paper form at any time upon request at the brainit.sk head office.

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

These GTC form an integral part of each Agreement and Agreement with CA. In the event of a conflict between the general conditions and the provisions in the contracts, the provision according to the contracts takes precedence.

For the provision of Trusted Services by the Provider and their acquisition by the Customer, depending on the type of Certificate provided, in addition to the stated GTC, the relevant Policy of the Provider is also binding.

The Provider informs each person interested in Trusted Services about the VP before entering a contractual relationship with the Provider. VP are also permanently accessible in electronic form on a durable carrier:

- on the website https://zone.nfqes.com
- in the process of applying for the issuance of the Certificate

The person interested in issuing the Certificate, who becomes the Holder of the Certificate, is forced to actively express his consent to these VPs after they are made available, i.e. by signing the application for the issuance of the Certificate with a qualified electronic signature through your electronic identity card (eID) with a qualified time stamp, which informs that by signing the application with a qualified electronic signature you express your consent to the VP. is informed immediately in the application. This qualified signature is subsequently validated, which verifies the validity of the signature, the validity and authenticity of the data and the validity of the identification documents. Subsequently, this request for the issuance of a Certificate with a qualified electronic signature and a qualified time stamp will be kept in the records of the RÚ. By signing and agreeing to these Terms and Conditions, the holder of the certificate automatically agrees to the principles of personal data processing according to the GDPR.

The signing of the application for the issuance of the Certificate by a qualified electronic signature of the applicant for Certificates, who subsequently becomes the Holder of the Certificate, is the subject of a contractual agreement on the provision of Trusted Services addressed to the Provider, the content of which consists of these General Terms and Conditions.

Acceptance of the proposal for the conclusion of the contract resulting from the previous paragraph by the provider and subsequently the conclusion of the contract between the provider and the holder of the certificate occurs at the moment of the provision of the required Trustworthy Service, i.e., the moment in which the required 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 General Terms and Conditions.

After concluding this contract according to the previous paragraph, the Provider will issue a Confirmation to the Certificate Holder. The holder of the Certificate is obliged to sign it with his qualified electronic signature.

The contract with the Customer, who is not the Certificate Holder at that time, will be concluded in writing and is not subject to the procedure according to the above paragraphs.

For the provision of Trusted Services by the Provider, in addition to the stated GTC, the Provider's Principles are also binding.

3. Services provided by brainit.sk

These GTC apply in the relationship between the Provider and the Participants, as well as in the relationship between the Provider and the Relying Parties in the provision of any of the Provider's trusted services.

3.1 Issuance of a qualified certificate for electronic signature

Qualified certificate for electronic signature in accordance with Art. 28 of Regulation (EU) No. 910/2014 is issued only to a natural person (holder), or a natural person authorized by the holder or a person acting on their behalf based on the law or a decision of the competent authority. Depending on the profile and issuing policy, the certificate can be used for authorship certification in 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 certificates for electronic signatures can also be used for signing document packages (ASiC-E) as well as e-mails (based on S/MIME (Secure/Multipurpose Internet Mail Extensions/Protocol for secure transmission of e-mails over the Internet or cryptographic system for the protection of messages transmitted by electronic mail and data stored on various media). The certificate may also contain data on a legal entity linked to a natural person on whose behalf the signing person is signing. In such a case, brainit.sk does not certify the representation of the Holder's natural person vis-à-vis the legal entity, but only that there is a legal relationship between the Holder and the legal entity.

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

3.1.1 QC issued for a natural person for QES

Issuance of a certificate is a qualified new application according to Regulation (EU) no. 910/2014. The certificate Qualified natural person for ZEP is issued for the purpose of electronic authorship of a natural person in documents signed electronically and to which the certificate is added, as well as to identify the holder with specific additional preparations described in the certificate. All rules and regulations for its issuance and management coincide with the certification policy for the provision of this certification service.

3.1.2 QC issued for a natural person for AES

The issuance of such a certificate is a qualified trusted service according to Regulation (EU) No. 910/2014. A qualified certificate for AES is issued in accordance with all policies and procedures for issuing qualified certificates according to 3.1.1.

3.2 QC issued for electronic seal

A qualified certificate for an electronic seal is issued to each subject (Customer) who is authorized to act on behalf of the given legal entity according to the applicable national legislation and can be used to guarantee the origin and integrity of the output data. of a legal entity, e.g.: electronic documents, photographs, architectural projects, software, etc. This trusted brainit.sk service is provided in accordance with Art. 38 of Regulation (EU) No. 910/2014. Profile types of qualified certificates for the electronic seal 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 trusted service according to Regulation (EU) No. 910/2014. The attribute in the certificate contains information that the certificate is qualified and shows whether a private key was used to create the electronic seal. Brainit.sk issues a certificate and delivers it to the person authorized by the legal entity. By accepting these GTC when requesting this service, it is deemed 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 trusted service according to Regulation (EU) No. 910/2014. A qualified certificate for AESeal is issued in accordance with all policies and procedures for issuing qualified certificates according to 3.2.1.

3.3 QC issued for authentication of website

A qualified website authentication certificate is issued for the purpose of certifying a website by a specific natural or legal person. The purpose is to assure 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 the exchange of information between the website and its visitors. This qualified, trustworthy service is provided by brainit.sk in accordance with Art. 45 of Regulation (EU) No. 910/2014.

3.4 QC issued for qualified timestamp

Issuance of a Qualified Electronic Time Stamp is a qualified, trustworthy service that brainit.sk provides in accordance with Art. 42 of Regulation (EU) No. 910/2014. Qualified electronic time stamps are issued to natural persons and legal entities. A qualified electronic time stamp assumes the correctness of the date and time indicated on it, as well as the integrity of the data sent to brainit.sk. Such data can be an electronic signature, an electronic seal, a hash of unsigned electronic documents or a hash of other electronic content.

A qualified electronic time stamp can be integrated into the process of creating, sending or receiving electronic signatures/seals, electronically signed documents and electronic transactions, when archiving electronic data, etc. This service uses the technology of binding date and time to data in a way that excludes the possibility of unobserved data changes and provides an opportunity in the following period (after the expiration of the Qualified Electronic Time Stamp) to prove the fact that the electronic document or other electronic item was signed at that time.

3.4.1 Specific requirements relating to relying parties

The primary responsibility 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 timestamp

(TSU/timestamp unit) as well as the validity period of this certificate. If timestamps are checked after the TSU certificate expires, the relying party must:

- check the time-stamped certificate in the Certificate Revocation List (CRL)
- check the applicability of the used hashing algorithm
- verify the security of the used electronic signature by checking the applicable combination of asymmetric and hashing algorithms

When relying on a qualified electronic timestamp, the relying party must:

- verify that the qualified electronic time stamp has been properly signed and that the private key used to sign the time stamp has not been compromised until the time of verification
- take into account all restrictions on the use of time stamps set forth in these Terms and applicable policies and procedures
- take into account all other measures prescribed in these terms and conditions and applicable 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 trusted service within the meaning of Art. 32, 33 and 40 of Regulation (EU) No. 910/2014. This service serves to verify electronic signatures, electronic seals, registered e-mail services and certificates related to these services issued and provided by brainit.sk. Verification also takes place through qualified website verification certificates. The qualified validation service is provided by brainit.sk as a qualified provider of trusted services and by providing it with a special document (result of the validation process) confirming the validity or results of the validation process.

In the process of verifying a qualified electronic signature/seal, the company brainit.sk confirms the validity of a 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) №910/2014
- The qualified certificate was valid at the time of signature

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

3.5.1 Purpose and limitations of service use

The purpose of the service is to provide a qualified, trustworthy service for verifying qualified electronic signatures and seals. The assumed way of using the service is its integration into the Applicant's process when verifying the validity of electronically signed documents or directly by the end user through the NFQES portal.

The service is provided in accordance with the requirements of the Regulation of the European Parliament and the Council (EU) no. 910/2014 of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS

Regulation). Law no. 272/2016 Coll. on trusted services for electronic transactions in the internal market and on amendments and additions to certain laws (Act on trusted services) and the Scheme of supervision overqualified trusted services defined by the supervisory authority - NBU 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 requirements for trust service providers".

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

The service can be used through predefined interfaces after the service has been made available by the Operator and exclusively for the defined purpose.

3.6 Qualified electronic mailbox service

A qualified registered mailbox service is a trusted service that enables the electronic transfer of data between third parties and provides proof of the identity of the sender and receiver of the transmitted data, the time of sending and receiving the data, and protects the transmitted data against the risk of loss, theft, damage, or unauthorized changes. The service provides:

- high degree of reliability of sender identification
- identification of the sender before data delivery
- secure sending and receiving of data through a guaranteed electronic signature or a guaranteed brainit.sk electronic seal in a way that excludes all possibilities of unobserved data changes
- any data change required for the purpose of sending or receiving data is clearly marked for the sender and recipient of the data
- the date and time of sending and receiving, as well as every data change is marked with a qualified electronic timestamp

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

This trusted brainit.sk service is provided in accordance with Art. 44 of Regulation (EU) 910/2014. Records of sent messages can be kept for 10 years in the Provider's storage. It can be provided to the contracting parties in accordance with the valid 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

- Successful delivery is considered if the content sent by the sender has left the sender's information system and is no longer under his 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, receiving an electronic message from the Participant's web browser through the portal on the brainit.sk backend (server) and receiving the sent message

in the virtual mailbox accessible in the recipient's account through the web portal is considered successful delivery.

- When using the qualified REM service, the time of receipt of the electronic message to the information system on the brainit.sk electronic mailbox server (backend) is considered to be successful sending, and receipt to the electronic mailbox operated by brainit.sk on the brainit.sk electronic mailbox server is considered to be received.

Brainit.sk ensures that the service protects transmitted electronic content from loss, theft, breach 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 Art. 34 and Art. 40 of Regulation (EU) No. 910/2014. These trusted services ensure safe and reliable long-term storage of all types of electronic signatures and seals attached to documents (without storing the documents themselves in a vault) and/or electronically signed/sealed documents (with a vault) of participants and provide records of the storage process with the possibility of long-term verification of electronic signatures/seals. The data objects, the relevant evidence of storage and the additional information necessary for their verification are available 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 reliably protected by encryption. In any case, they will be handed over only to the Participant or his authorized representative. Brainit.sk stores 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 state the person requesting the data, the reasons for their request and the way they wish to receive it, for example by e-mail or on an electronic medium. The company brainit.sk reserves the right to approve or reject the implementation of the application without having to justify its rejection or inform the applicant about it, except for cases specified in the legislative act. To provide data and evidence, brainit.sk may collect fees for ensuring the processing of the submitted application. 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 the provision of the Trusted Service is determined in accordance with the Price List, which is valid during the provision of the Trusted Service, unless the contracting parties agree otherwise.

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

The Customer is obliged to pay the value of the price for the Trusted Services by non-cash transfer based on the invoice issued by the Provider after the requested Trusted Service has been provided. The due date of this invoice is 2 weeks t. j. 14 days, unless generally binding legal regulations or the given contract stipulate otherwise. The price for these Trusted Services is considered paid on the day this amount is credited to the Provider's bank account in full.

It is necessary that the invoice issued by the Provider contains all the details of the tax document listed in § 74 par. 1 of Act no. 222/2004 Coll. on value added tax as amended. The Customer has the right to object to the Provider about the content or formal deficiencies of the invoice within its due date. The Provider will evaluate the Customer's objections and, if they are justified, will subsequently issue a new invoice, the due date of which will start from the date of its delivery to the Customer.

If the Customer does not pay the full amount for the provided Trusted Services within the due date according to the GTC or the given contract, the Trusted Services Provider has the right to immediately withdraw from the contract, which also results in the cancellation of any certificate for which payment has not been received.

5. Issuance of certificates

Certificates according to the above VP are issued exclusively on the HSM device, remotely mediated by the Application, only based on the request of the person interested in the Certificates. In case of fulfillment of the conditions determined by these VP and the Policy of the Provider, the Provider is obliged to issue the Certificate to the Holder and deliver it as soon as possible. At the same time, the Provider issues a Confirmation of issued Certificates, which is signed by the Certificate Holder. The confirmation is determined by the specific Certificate that was issued for the Certificate Holder. A reliable service is considered to have been provided at the moment of acceptance 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 damages resulting from the use of services exceeding the limitations of their use specified in these GTC. Relying parties agree and undertake to take all necessary precautions when relying on the electronic identification service or the trusted service provided by brainit.sk to monitor and comply with the restrictions on the use of services specified in these GTC.

5.1.1 Time limits

Each certificate issued by brainit.sk can only be used until its validity expires. The period of validity of the certificates is indicated in it. If the certificate has been revoked, the signer/creator may 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 purpose, as described in these GTC, in the relevant principles and procedures of brainit.sk and in the relevant law. Verification of the intended purpose of the certificate is carried out based on the data provided in the certificate profile:

- the policy/practice in accordance with which the electronic signature/seal certificate is issued and managed
- the 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 together with the corresponding pair of keys can be used in the usual way, only for the purpose for which it is intended in accordance with the conditions and restrictions stated in the relevant Policy of the Provider. The certificate is intended exclusively for the creation of an electronic signature or improved electronic signature of the Certificate Holder. Since the

Device is a qualified device according to the eIDAS regulation, it is possible to create a qualified electronic signature using the Certificate.

The period of validity of the Certificates is limited. After the expiration or cancellation of the Certificate, it is prohibited to use the Certificate, even for the purpose specified by it. As a result of the use of an invalid or canceled Certificate, which is also intended for creating an electronic signature, this electronic signature will subsequently be invalid as well.

The verifiability of an electronic signature has limitations, i.e., after the expiry of the validity of the Certificate based on which they were drawn up, it is not guaranteed that it will be possible to verify the validity of the electronic signature in question. To ensure the long-term verifiability of this electronic signature even after the expiration of its validity period, based on which it was created, it is necessary to use specialized services in an appropriate way even during the validity of this electronic signature Certificate such as an electronic signature storage service and/or an electronic time stamp service.

Using the Certificate to create an electronic signature does not guarantee that the created electronic signature can be used for the intended 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 GTC or relies on the Certificate in violation of these restrictions and he or a third party incurs damage in connection with this action, the Provider is obliged pursuant to Art. 13 par. 2 does not comply with the eIDAS regulation.

7. Specific conditions for issuing qualified trust services

7.1 Acceptance of the certificate

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

If the certificate contains incorrect information, the certificate will be revoked immediately. If the Participant objects within 3 (three) days of publication in the certificate repository that the issued qualified certificate contains errors or deficiencies, brainit.sk will remove it free of charge by issuing a new certificate, unless these occur as a result of providing incorrect data. If no objections have been raised, the content of the certificate is considered accepted. The rules stated in this point apply both to the issuance of the certificate and to the renewal of the certificate.

A qualified certificate is considered accepted by the participant if any of the following conditions are met:

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

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

8. Rights and obligations of the customer and certificate holder

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

If the Customer is a consumer, in the event of defects in the Trustworthy Service, he has rights according to § 622 and § 623 of the Civil Code.

In particular, the customer is obligated to:

a) provide the Provider with all the data and documents necessary in accordance with the Provider's Principles to provide the requested Trustworthy Service, while the data and documents must be true, up-to-date and complete;
b) in the case of providing data that is necessary for the provision of the Trusted Service, ensure in advance that this data is sent to the Provider in a way that guarantees its confidentiality and integrity (e.g., sending an encrypted file electronically and sending the password via a special channel);
c) use the Certificate and the generated pair of keys only for the purposes intended for it in accordance with the legal regulations and restrictions on their use specified in the GTC;
d) when using the Certificate and relying on the Certificate, proceed with caution according to part 10 of the GTC;
e) refrain from unauthorized use of the Certificate Holder's private key if the Customer and the Holder are not the same person;
f) in cases where the Customer generates cryptographic keys for which a Certificate is to be issued, he is obliged to create a key pair of a prescribed length using the algorithm required by the Provider's Policy applicable to the requested Certificate;
g) enable the use of the private key for which the Certificate is issued for cryptographic functions exclusively within the Device and under the sole control of the Certificate Holder;
h) provide the Provider, upon request, with immediate and timely cooperation in verifying the data necessary for the issuance of the Certificate;
i) during the validity of the Certificate, immediately notify the Provider of changes, errors or outdated data in the Certificate;
j) during the validity of the Certificate, immediately notify the Provider if there is misuse, theft, loss, impairment, destruction, endangerment or any unauthorized access to the related private key or access codes (password and token) or if the Customer suspects that the above may occur events; and ensure that the Certificate Holder refrains from using the private key and the expired certificate is revoked or compromised (even if the Provider itself was attacked and the Customer knew about it).

The Holder of the Certificate has the right to use the Certificate issued by the Provider in accordance with the contract and these General Terms and Conditions.

The holder of the certificate is obliged in particular to:

a) immediately after obtaining the Certificate, check the correctness and up-to-dateness of the data in it and always provide only true and up-to-date data and documents in connection with the Trusted Services;
b) when using the Certificate and relying on the Certificate, proceed with reasonable care in accordance with part 10 of these GTC;
c) use the Certificate and the generated pair of keys exclusively for the purposes intended for it in accordance with generally binding legal regulations and restrictions on their use specified in the GTC;
d) protect the access code (password and token) against unauthorized access and also against loss, disclosure, destruction or misuse;
e) during the validity of the Certificate, immediately notify the Provider of changes, inaccuracies or out-of-date data, which are stated in the given Certificate;
f) during the validity of the Certificate, immediately notify the Provider if there is misuse, theft, loss, destruction, endangerment or any unauthorized access to the assigned private key, access code (PIN), renewal code (PUK) or to the device on which the keys are stored , or if the certificate holder suspects that the mentioned events may have occurred and refrains from using the private key and certificate whose validity period has already passed, which has been revoked or is at risk (including if the provider has been attacked and the certificate holder knows about it).

The Customer or the Holder of the Certificate of the Provider requests the cancellation of the Certificate through the contact details specified in Art. 3 VP.

9. Rights and obligations of the provider

The Provider is entitled not to provide the Trusted Service, or to limit the scope of its provision to the client (e.g., by not specifying all the required attributes in the Certificate), if the conditions for issuing the Certificate, which are defined in the Provider's Policy or in this document.

The Provider is entitled to cancel the Certificate in the cases specified in the relevant Provider Policies, especially if:

a) acknowledges that the conditions of the eIDAS Regulation, the Act or the Provider's Principles were not met for the issuance of the Certificate;
b) discovers that the Device on which the keys or its software components are stored are or may be hacked;
c) the court orders him to cancel the Certificate;
d) The Customer has not paid him the agreed price of the Trusted Services within the predetermined deadline, even on the basis of a request sent electronically by the Provider;
e) The customer shall not publish the contract with the Provider within three months of its conclusion in cases where it is a contract that needs to be published in accordance with § 5a of Act no. 211/2000 Coll. on free access to information and on the amendment of certain laws (the Freedom of Information Act);
f) there is termination or termination of the contract with the Customer or the Certificate Holder or if the Certificate Holder does not sign the Confirmation;
g) The Customer or the Certificate Holder violates the given obligations in terms of these General Terms and Conditions, the contract or generally binding legal regulations;

h) becomes aware of any changes affecting the validity of the Certificate, especially in cases where the information provided in the Certificate is false or out of date or becomes aware of theft, loss or endangerment of access codes, etc.;
i) discovers that the Customer or Certificate Holder has died (in the case of a natural person) or has ceased to exist (in the case of a legal entity);
j) cancellation is requested by the Customer or the Certificate Holder;
k) the certificate no longer complies with the policy on the basis of which it was issued;
l) the cryptography used for the given Certificate no longer ensures the connection between the Holder of the Certificate and the public key.

The Provider is entitled to publish the name of the Customer on its website as a reference unless the contract stipulates otherwise.

The Provider is obliged to provide Trusted Services in accordance with the eIDAS Regulation, the law and its own Principles valid at the time of their provision.

10. Information for parties relying on trust services

Relying Parties acknowledge that it is solely at their discretion whether they choose to trust and rely on the Certificate issued by the Provider and the information contained therein. In the event of a decision to rely on the Provider's Certificates, it is the duty of the relying parties to comply with the obligations described in this Part 10 of the GTC, otherwise they are solely responsible for the legal consequences caused by this.

The Relying Party acknowledges that the validity of Certificates, CRLs as well as OCSP responses issued by the Provider is limited in time:

a) The certificate is in the body of the certificate during the period of validity or until the moment of its cancellation before the valid period of validity;
b) The CRL is valid during the period of validity of the physical CRL, while in order to obtain the most accurate information about revoked Certificates, it is necessary to always use the most current CRL, i.e.;
c) The OCSP response is valid at the time indicated by the item "madeAt" in the body of the OCSP response. The ProducedAt field is only the signature time of the OCSP response and has nothing to do with the valid certificate.
d) Only such CRL and OCSP responses can be used to verify the signature or verification, where the thisUpdate item contains a time and date after the time and date of the signature, which is in the interval of validity of the certificate and is considered to be the time when the validity of the certificate lasts.

The Relying Party is obliged to exercise reasonable care to be able to rely on any Certificate issued by the Provider, in particular it is obliged to:

a) evaluate whether the use of the Certificate is in accordance with its purpose and whether it is suitable for the given purpose;
b) check whether the use of the Certificate does not conflict with the restrictions on the use of the Certificate specified in the Certificate itself, in these General Terms and Conditions or in the Provider's Policy, which are linked to the given Certificate;

c) use only appropriate hardware or software when working with the Certificate, including its verification;

d) verify the validity of the Certificate in question using an application validating a qualified certificate using a list of trusted published NBUs and a corresponding CRL or OCSP response with thisUpdate item indicating the time and date after the signature or seal was created;

e) if necessary, perform additional verifications that may be required in terms of the Provider's Principles or standards for a specific type of Certificate or its use;

f) in the manner according to points a) - e) verify also other certificates on the certification path up to the so-called "anchor of trust". The trusted anchor is stored in the trusted list published by the NBU. Certificates stored in a trusted list represent an "anchor of trust".

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

To rely on a CRL or OCSP response issued by the Provider, it is the duty of the relying party to exercise reasonable care. In particular, the obliged party is obliged to verify that the certificate with which the CRL or OCSP response was signed belongs to the Provider using the list of trusted information issued by the NBU and at the same time proceed similarly according to Art. 10 of these General Terms and Conditions.

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

For damage caused by non-fulfillment of obligations under the eIDAS Regulation according to Art. 13 eIDAS regulations.

The Provider is obliged to provide Trusted Services in accordance with generally binding legal regulations and the Provider's Principles. He is responsible for defects in the provided Trustworthy Service in accordance with generally applicable legal regulations.

The Provider is not responsible for indirect losses or damages incurred by the Customer, Certificate Holder, Relying Party or third party in connection with the use of Trusted Services.

The Provider is not responsible for damage (including lost profit) incurred by the Customer, the Certificate Holder, the Relying Party or any third party as a result of:

a) violation of the obligations of the Customer, the Certificate Holder or the Relying Party specified in the generally binding legal regulations, these GTC, in the relevant contract or in the Provider's Principles, including the obligation to provide reasonable care when using the Certificate and relying on the certificate;

b) failure to provide the necessary cooperation on the part of the Customer or the Certificate Holder;

c) technical characteristics, configuration, incompatibility, inappropriateness or other errors of the software or hardware used by them;

d) using or relying on an expired or revoked certificate;

e) The Certificate was used in violation of the purpose or restrictions stated in the Certificate, in these Terms of Use or in the Provider's Policy;

f) delay or non-delivery of requests to verify the status of the Certificate to the Provider, for reasons not attributable to the Provider (especially cases of unavailability or overload of the Internet or non-functionality of equipment or technical devices used by the Provider);

g) failure to provide any of the Trusted Services or its unavailability during planned maintenance or reorganization announced on the Provider's website;
h) acts of force majeure.

The Provider is not responsible for damages caused to the Relying Party by not proceeding in accordance with point 10 of these GTC when relying on the Provider's Trusted Services or on an electronic signature or seal created on their basis.

The provider is also not responsible for:

a) for the fact that an unauthorized person took possession of the Customer's or Holder's access codes;
b) for damages caused by the use of the Certificate, if the Customer or the Certificate Holder does not act in accordance with their obligations, especially if an unauthorized person gains access and the Customer or the Certificate Holder does not act to request the Provider to cancel the Certificate or if they do not notify the Provider of data changes;

The Customer and the Certificate Holder use the Trusted Services at their own risk and bear all costs for means of remote communication or other technical means necessary to use the Provider's Trusted Services (e.g. for the software required to create an electronic signature or seal based on the Certificate);

12. Protection of privacy and personal data

12.1 Processing of personal data

Brainit.sk carries out its activity of providing trustworthy services in accordance with the requirements of Regulation (EU) 2016/679 (GDRP), applicable legislation and in accordance with its applicable Personal Data Protection Principles, which are an integral part of these General Terms and Conditions and the contract with the Participant.

Valid personal data protection principles of brainit.sk include:

- Personal data protection policy valid for trusted, informational, cryptographic and other services provided by Brainit.sk (all services)
- Other personal data protection principles that brainit.sk may adopt and apply in connection with the provision of some of its services

The personal data protection principles applicable to trusted, informational, cryptographic and other services provided by brainit.sk apply to the activities performed during the provision of services according to these GTC. In connection with some of its services, the brainit.sk company may also ensure and implement special personal data protection principles regarding the processing of personal data by the brainit.sk company when providing these services. In the event of a conflict between the Personal Data Protection Principles, which apply to trusted, informational, cryptographic and other services provided by brainit.sk, and these special principles, the special principles take precedence, but only with regard to processing activities related to the processing of personal data. provision of relevant services to which these principles apply. In case of gaps in the special principles, the provisions of the personal data protection principles apply, which apply to trusted, informational, cryptographic and other services provided by brainit.sk.

Before concluding the contract, the Participant familiarizes himself with the Personal Data Protection Principles, which apply to the services requested by the Participant, in order to find out in what way, what type of personal data and for what purposes brainit.sk processes them. , as well as being informed about your rights and all other important issues related to the protection of personal data in accordance with the GDPR.

The provision of services is inherently related to the reception, transmission, storage, and processing of the Participant's data through the brainit.sk systems, to dependent persons, as well as to the exchange of this data between them and the provider in accordance with applicable legislation. and contractual relationships between all the persons. The participant is considered familiar with the above and agrees that his data will be provided to third parties for the purpose of providing services.

The provider processes the personal data of the affected persons in accordance with the relevant legal regulations. The provider can provide this data to third parties if they request it or if the relevant legal regulations allow it.

To informing affected persons or those interested in Trusted Services about the processing of personal data carried out by the Provider when providing Trusted Services, the Information on the processing of personal data serves:

a) always available in electronic form online at https://nfqes.com
b) about which the Certificate Holder is informed in the process of applying for the issuance of the Certificate

The Provider records and archives all relevant information and documents related to the issuance or cancellation of the Certificate and based on which the Certificate was issued, including the personal data of the Customer, the Certificate Holder, or persons authorized to act on their basis on behalf of or authorized VPs for a period of 10 years from the date of cancellation or expiration of the Certificate in question.

The holder of the Certificate acknowledges that if the electronic document is signed based on the Certificate intended for this purpose, the recipient of this electronic document or persons who have or will have access to this electronic document will gain access to their personal data listed in the list. in the Certificate.

13. Resolution of disputes and complaints

The user is entitled to send a complaint, initiative, or complaint to the Provider of trusted services by email to ca@nfqes.sk. The provider will respond to it within 30 days of its delivery, in the case of more complex complaints or claims, it reserves the right to extend this period.

The courts of the Slovak Republic are exclusively competent to decide any disputes between the Provider and the Customer, or the Holders of the Certificate. In the event that the Customer or Certificate Holder is a consumer, he is entitled to turn to an out-of-court dispute resolution entity, e.g. Slovak Trade Inspection or other legal entity entered in the list according to § 5 par. 2 of Act no. 391/2015 Coll. on alternative resolution of consumer disputes, as amended. Before proceeding to judicial or extrajudicial dispute resolution, it is the duty of the contracting parties to try to resolve the dispute by mutual agreement in advance.

14. Governing law

Legal relations between the Provider and the Customer or Certificate Holder are governed by the legal order of the Slovak Republic.

Legal relationships not expressly regulated by these general terms and conditions, or the contract are governed by the relevant provisions of Act No. 513/1991 Coll. Commercial Code as amended and other generally binding legal regulations. If the Customer or Certificate Holder is a consumer, the provisions of Act No. 40/1964 Coll. 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 expiration or cancellation of the Certificate to which the contract applies.

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

a) based on the mutual agreement of the contracting parties;

b) based on the termination of one of the contracting parties regarding the contract concluded 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 contracting party;

c) withdrawal from the contract by one of the contracting parties in the event of a material breach of contractual obligations by the other contracting party.

A substantial breach of contractual obligations, which establishes the right to withdraw from the contract, is:

a) if the Customer does not pay the full price for the provided Trusted Services within the agreed deadline;

b) if the Certificate Holder or the Customer uses the Certificate in a way that is contrary to legal regulations, these VP or the Provider's Principles;

c) if the Customer or the Holder of the Certificate violates the obligation to request the cancellation of the Certificate in the cases determined by these VP or the contract;

d) for other reasons in accordance with the generally binding legal regulations of the Slovak Republic.

If the Provider uses its right to withdraw from the contract, it also has the right to cancel the Certificate, the violation of which by the Customer or concerns the holder of the Certificate.

In the event of termination of the contract, the Customer's obligation to pay any debts incurred in connection with the use of Trusted Services shall not cease.

Termination of the contract between the Provider and the Customer, or It does not apply to the holders of the Certificate on those provisions, from the nature of which it follows that they should continue even after their termination.

15.1 Contract, conclusion, subject of contract

The company brainit.sk will provide free of charge or for a fee the services to which these General Terms and Conditions apply, provided that the participant/signatory/creator of the contract concluded in accordance with these General Terms and Conditions, as well as in accordance with applicable legal regulations, strictly complies. The services are diverse, constantly supplemented and modified with the aim of improving and expanding them, and based on this, brainit.sk can at any time unilaterally change their number, features, and conditions of their provision within the limits set by applicable legislation.

Brainit.sk services can be requested or provided in different ways depending on their nature and in accordance with these GTC. The request for the service and the conclusion of the contract requires the secure identification of the Subscriber in accordance with the level of security required for the specific service and the Subscriber's agreement to these GTC. Before requesting the service, the Participant familiarizes himself with all the Principles and procedures applicable to the relevant service. By requesting the service, the Subscriber accepts these GTC.

Different brainit.sk services can be requested in different ways, and not every inquiry method provides the possibility to request each of the services. Brainit.sk maintains up-to-date information on its website about ways to request and use different types of services.

Brainit.sk services can be requested in one 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 on 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 an authorized representative duly authorized to represent. , if the Participant is a legal entity.

For a natural person:

For clear identification and identity verification, the participant will provide the following data:

full name (as in the identity document); identity document – identity card, international passport, or other identity document; national identification number, if any; contact details - mobile phone number, e-mail address and postal address. A copy of the identity document is not made. After successful verification of the Participant's identity, an authorized operator from the internal Registration Authority brainit.sk:

- draw up a contract on qualified trusted services signed on behalf of brainit.sk and keep all submitted documents related to the contract. The Agreement shall be signed by the Participant in written form together with these General Terms and Conditions, the applicable Personal Data Protection Policy of brainit.sk and all other documents relevant to the requested service.
- confirms the request for issuance and sends the electronic request for the issuance of the certificate to the operational certification authority brainit.sk;
- records the issued certificate on a secure signature creation device and delivers it to the signer or authorized person (if relevant).

With a legal entity:

Establishing the identity of a legal entity is carried out by the RA by verification in the relevant registers based on the provided registration or other unique identification number of the legal person. Identification of the legal person and verification of the authorized representative is carried out on the spot based on the information provided by the Participant through documents sent remotely or through a personal meeting. Such identification verifies all the data that will be listed in the issued certificate, as well as the authorization of the legal representative of the person who attended the physical meeting at the brainit.sk headquarters.

In the case of legal person, it is necessary to submit:

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

After all required documents have been copied 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 according to Regulation (EU) No. 679/2016, but contractual consent is a mandatory condition for concluding a contract. The verification of the data contained in the submitted documents is carried out by verifying the "true copy or original" and the handwritten signature signed by the person representing the Participant in front of the RA employee. The legal person identity certificate has two purposes: (1) verifying whether or not the legal person exists at the time of the request review, and (2) verifying that the person acting on behalf of the legal person has the necessary representative authority to request the relevant trusted services and validly conclude a contract on behalf of the Participant on their provision according to these GTC.

15.1.2 By personally visiting the external Registration Authority brainit.sk

The process of requesting a service and concluding a contract begins with a personal meeting of an individual Participant or a legal representative or a duly authorized representative of a legal entity of the Participant at the workplace of the external Registration Authority and applying for Registration. Authorization for the relevant service. The application can be submitted to the external brainit.sk registration authority for any of the brainit.sk services, in connection with which the relevant external registration authority is authorized to act as the brainit.sk registration authority. After sending the Participant's request to the Registration Authority, the same service request procedure as described above in this section will be performed.

16. Final provisions

The Provider is entitled to unilaterally change the General Terms and Conditions or the Price List, for reasons based on the business policy of providing Trusted Services, for reasons of changes to generally binding legal regulations, changes to standards governing the provision of Trusted Services, e.g. reasons for technical, security or organizational changes in the systems used to provide Trusted Services on the Provider's side, as well as for the purpose of increasing the quality, security or availability of Trusted Services. In such a case, he is obliged to notify the Customer and Certificate Holders of a change in these documents at least 30 days before the effective date of these changes, by sending an informative electronic message to the above-mentioned email address and by publishing them on the Provider's website. If the Customer or the Certificate Holder does not agree to the change of the binding document, they have the right to terminate the contract with the Provider with immediate effect within 30 days of sending this information to the Provider. The termination can be sent to the address of the Provider's registered office or to the email address info@nfqes.sk. If the Customer or Certificate Holder does not reject the proposed change in writing no later than on the effective date of the change in question, it is considered that he agrees with it and this change becomes binding for him from the effective date.

For the delivery of legal acts and other legal acts between the Provider on the one hand and the Customer, or Certificate Holders on the other hand, the contact data that the contracting parties have provided to each other, especially the email address and the address of the company's headquarters, are required. place of residence, are used. It is the duty of the contracting party to immediately notify the other contracting party of any changes to its contact details. Until the moment of notification of the change of contact data to the other contractual party, the provided contact data are considered to be true.

If any provision or part of these GTC or contract is or becomes invalid or ineffective, this does not affect the validity and effectiveness of any other provision or the remaining part of the relevant provision. The contracting parties undertake to replace such an invalid or ineffective provision with a provision on which they would have agreed if they had known about this invalidity or ineffectiveness.

If any provision, part thereof 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 provision of the general terms and conditions shall not be affected thereby.

These General Terms and Conditions are valid and effective from July 20, 2023.