

CONTRACT FOR THE PROVISION OF QUALIFIED ELECTRONIC SIGNATURES WITH ONE-TIME OR TIME-LIMITED VALIDITY

I. Subject of the Contract

Art. 1. (1) The PROVIDER shall provide the Signatory with a cloud-based qualified electronic signature (CQES), with a validity limited to 1 (one) hour that can be used to sign documents related to a service provided by a Relying Party.

(2) An application for the service referred to in Art. 1, paragraph 1, shall be made using the PROVIDER's application form that is attached to this Contract and constitutes an integral part of it.

(3) The PROVIDER's Policies and Practices for the provision of the service referred to in Art. 1, paragraph 1, Information to the Owner of the Personal Data, the General Terms and Conditions for the Use of the B-Trust Mobile Application, the Installation Guide for the B-Trust Mobile Application and the PROVIDER's Tariff for the Provision of Trust Services, are an integral part of this Contract, hereinafter referred to as the "Contract". The latest version of these documents is available on the following website: <https://www.b-trust.bg/documents>.

(4) The PROVIDER shall publish on the website referred to in paragraph 3 of this article the following information:

- The scope of the services offered;
- Instructions for using the services.

II. Conclusion and Duration of the Contract

Art. 2. (1) The duration of this Contract is 24 (twenty-four) hours from the moment of its conclusion.

(2) With the first CQES issued under this Contract, the Signatory shall electronically sign the Contract and its Appendix, thereby completing the process of entering into the Contract. Once the Contract is signed, the one-time CQES will be activated and will be available for use by the Signatory.

(3) The procedure for requesting the first one-time CQES issued under this Contract shall include the identification of the Signatory. Each subsequent one-time CQES issued under this Contract shall be issued with the data provided and verified during the identification of the Signatory.

(4) To conclude the Contract, the Signatory must provide a valid mobile phone number, which is necessary to receive an SMS with a password to confirm the issuance of each one-time QES.

(5) The one-time CQESs issued may only be used for the one-time signing of documents that are associated with the specific service for which they were issued.

III. Rights and Obligations of the Parties

Art. 3. (1) The PROVIDER may request information and documents, necessary for the issuance of certificates in order to identify the Signatory and verify the data provided by the Signatory during the processing of the application for issuance of the Certificate(s) by the Registration Authority.

(2) The PROVIDER may only publish information about the Signatory contained in the issued certificate unless public access to the contents of the certificate is restricted at the request of the Signatory.

(3) The PROVIDER shall notify the competent authorities in case of reasonable suspicion of unlawful activities of the Signatory for the purpose of or in connection with the provision of the Services.

Art. 4. (1) The PROVIDER agrees to:

1. issue a certificate to the Signatory and promptly publish it in accordance with the Signatory's instructions;
2. inform the Signatory of the terms and conditions of issuance and use of the certificate;
3. provide access to the private key for use of the certificate only to the Signatory;
4. not store unencrypted data related to the generation of the private key;
5. immediately terminate the validity of the certificate if grounds for termination are found and in accordance with the applicable law and the provisions of this Contract and its appendices;
6. immediately notify the Signatory of any circumstances relating to:

CONTRACT/APPLICATION FORM
FOR A ONE-TIME QUALIFIED ELECTRONIC SIGNATURE FOR A LIMITED PERIOD OF TIME

- the validity or reliability of any issued certificate;
 - security breaches or other malicious actions related to the services provided or personal data stored that may cause damage and/or have a negative impact on the Signatory.
7. make available to third parties only the information contained in the certificate, while complying with the request made by the Signatory, unless otherwise provided by the policies and practices for the service;
8. issue a new certificate to the Signatory in the event of errors and/or omissions in the certificate issued, without requiring the payment of any compensation, unless the errors and/or omissions are the result of incorrect, incomplete or inaccurate data provided by the Signatory;
9. publish and update electronically a public list of revoked certificates of the Provider;
10. publish on the website referred to in Art. 13, paragraph 2, a current version of the documents referred to in Art. 1, paragraph 3 of this contract;
11. ensure the implementation of technical and organizational measures related to the security of the services provided;
12. ensure the lawful processing of personal data in accordance with Regulation (EU) № 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Art. 5. The Signatory agrees to:

1. provide the PROVIDER with accurate and complete information that unambiguously identifies the Signatory and does not violate the rights of third parties to trade names, trademarks, domain name rights or any other intellectual property rights;
2. protect the private key throughout the life of the certificate in a manner that protects it from compromise, loss, disclosure, modification, and unauthorized use. From the time the key pair is created, the Signatory is solely and personally responsible for the secrecy and integrity of the private key. Any use of the private key shall be considered an act of the Signatory;
3. request the PROVIDER to immediately suspend or revoke his/her certificate in all cases where its immediate suspension or revocation is required by the EDE TSA;
4. immediately notify the PROVIDER of any change in the data and circumstances declared at the time of the issuance of the certificate or contained therein, and to request the immediate revocation of the certificate. In the event of a change in the circumstances stated in the certificate or the occurrence of other circumstances that require the revocation of the certificate, the Signatory shall immediately request the revocation of the certificate;
5. use the issued certificate only with licensed software;
6. use the certificate only for its intended purpose and in accordance with the limitations set forth in the certificate, this Contract and the appendices hereto;
7. observe the provisions of this Trust Services Contract, the documents referred to in Art. 1, paragraph 3 of the Contract and the applicable legislation;
8. pay the agreed price.

IV. LIABILITY OF THE PARTIES. LIMITATION OF LIABILITY

Art. 6. (1) The PROVIDER shall not be held liable by the Signatory or any third relying party for any damage caused by the Signatory's failure to comply with the obligations and responsibilities set forth in Art. 5 of this Contract.

(2) The PROVIDER shall not be held liable by the Signatory or any third relying party in case of:

- the inability to perform the obligations of the Contract due to technical problems (equipment or telecommunications) beyond the control of the PROVIDER, including physical damage, blocking or inability to access a smart card or reader;
- inappropriate authorization of a person to hold a private key corresponding to the public key that is certified in the Certificate issued under this Contract;
- failure to comply with the security requirements established by the PROVIDER, including the use of non-authentic software on the device and the use of a device with reduced security, regardless of the cause;
- occurrence of damages resulting from the use of the services in a manner that exceeds the limitations of which the Signatory has been previously informed by means of this Contract and its appendices;
- damage to software, hardware, telecommunications equipment and/or loss of data caused by materials or resources uploaded through the Mobile Application or through the use of a Service that is the subject of this Contract;

(3) The Signatory shall be liable to compensate the PROVIDER for all damages and loss of profit suffered by the PROVIDER as a result of the Signatory's failure to comply with its obligations under this contract, its appendices and current legislation.

CONTRACT/APPLICATION FORM
FOR A ONE-TIME QUALIFIED ELECTRONIC SIGNATURE FOR A LIMITED PERIOD OF TIME**V. PRICES AND PAYMENT**

Art. 7. Unless otherwise agreed, the fees for the use of the certificate referred to in Art. 1 shall be borne entirely by the Relying Party for whose purpose the certificate was issued.

VI. TERMINATION OF THE CONTRACT

Art. 8. (1) This Contract shall terminate:

1. at the end of the term specified in Art. 2 paragraph 1;
2. if it is found that the certificate was issued on the basis of untrue information provided by the Signatory, or on the basis of information withheld by the Signatory;
3. in the event of the death or placement under prohibition of the Signatory;
6. in case of force majeure;
7. in case of failure of the Signatory to comply with the obligations set forth in this Contract and its appendices;
8. by order of a competent authority;
9. in the cases provided for by the law.

(2) Upon termination of the Contract under the terms and conditions of paragraph 1, the validity of the Signatory's applicable certificate(s) of the Signatory shall terminate.

VII. ADDITIONAL PROVISIONS

Art. 9. By signing this Contract, the Signatory declares that:

1. is aware of the PROVIDER's registration as a Trust Service Provider;
2. has been informed by the PROVIDER of the conditions for issuing and using the certificates, including the limitations on their validity, and the procedures for filing complaints and settling disputes;
3. all information provided to the PROVIDER in connection with the issuance of the certificates, as well as the information contained herein, is true, accurate and complete, and that it will promptly notify the PROVIDER upon the occurrence of any change in the information provided or contained in the issued certificate;
4. is aware of the provisions of the applicable laws and the policies and practices of the PROVIDER for the provision of qualified trust;
5. is familiar with the contents of the appendices to this Contract, which are in force at the time of the conclusion of this Contract.

Art. 10. (1) This contract may contain special conditions that take precedence over the documents referred to in Art. 1, paragraph 3 of this contract.

(2) The invalidity of one or more provisions of this Contract or its appendices to it shall not affect the validity of the remaining provisions. In case of invalidity of one or more provisions, the existing legislation shall apply.

Art. 11. (1) This Contract shall be effective from the time the text of the Contract proposed by the PROVIDER is signed by the Signatory with a QES.

(2) The parties shall settle all disputes that may arise in the performance of this Contract amicably and in good faith and, if this proves impossible, in accordance with the provisions of law.

Art. 12. For all matters not provided for in this contract, the provisions of the legislation in force shall apply.

Art. 13. In the interpretation of the Contract and its appendices, the following terms shall have the following meanings:

1. **B-Trust Mobile** is a mobile application owned by BORICA AD and intended for the use of cloud qualified trust services.
2. **BORICA AD** is a company registered in the Commercial Register, maintained by the Registry Agency, under UIC 201230426 with its registered office and seat at the following address: 41, Tsar Boris III Blvd., Krasno Selo district, city of Sofia 1612, phone: 0700 199 10, e-mail address: office@borica.bg, certified for compliance with Regulation (EU) 910/2014, providing qualified trust services, entered in the national trusted list of qualified trust service providers, maintained by the Telecommunications Regulatory Commission (TRC), as part of the overall trusted list of all EU Member States. BORICA AD is a registered entity under the Value Added Tax Act and a controller of personal data under the Personal Data Protection Act.

CONTRACT/APPLICATION FORM
FOR A ONE-TIME QUALIFIED ELECTRONIC SIGNATURE FOR A LIMITED PERIOD OF TIME

3. **Electronic document** is any content stored in electronic form, in particular text or sound, visual or audiovisual recordings.
4. **Qualified Trust Service PROVIDER** is a PROVIDER of certification services that provides one or more qualified trust services and that has been granted its qualified status by a supervisory authority.
5. **Signatory** is a natural person who creates an electronic signature, as well as a natural person registered in the B- Trust Mobile application who has concluded a contract with the PROVIDER for the use of certification services provided by the PROVIDER.
6. **Relying Party** is any natural person or legal entity other than the Client, as well as any public entity, that relies on an electronic identification, authentication or other service provided by the PROVIDER.
7. **Fortuitous event** is a circumstance of an extraordinary nature, unforeseeable at the time of the conclusion of the contract, which makes the provision of the services objectively impossible.
8. **Website** is a reserved space on the World Wide Web, accessible through its unique address (URL) using HTTP, HTTPS or other standardized protocol, and containing files, programs, text, sound, image, picture or other materials and resources.
9. **Malicious acts** are actions or omissions that violate Internet ethics or cause damage to persons connected to the Internet or any related networks, sending unsolicited mail (unsolicited commercial messages, spam, junk mail), flooding communication channels, gaining access to resources using someone else's rights and passwords, exploiting vulnerabilities in systems for personal gain or to obtain information (hacking), Engage in activities that may be classified as industrial espionage or sabotage, damage or destroy systems or data arrays (cracking), send "Trojan horses" or cause the installation of viruses or remote control systems, disrupt the normal operation of other users of the Internet and related networks, or engage in any other activity that may be classified as a crime or administrative violation under Bulgarian law or any other applicable law.

CONTRACT/APPLICATION FORM
FOR A ONE-TIME QUALIFIED ELECTRONIC SIGNATURE FOR A LIMITED PERIOD OF TIME

**QUALIFIED ELECTRONIC SIGNATURE
WITH ONE-TIME OR TIME-LIMITED VALIDITY
APPLICATION FORM**

Registration number:	
Date:	
Time:	
Contract number:	

The Signatory consents to the collection, storage and processing of his/her personal data by the Provider and declares to have been informed that the Provider will use such data for the purposes of its activity as a provider of certification, information, cryptographic and consulting services, and will process and store such data in electronic and written form. The provision of personal data under Regulation 2016/679 of the EP is mandatory. The provision of personal data outside the scope of the Provider's activities is voluntary. The only recipients to whom the data may be communicated are the Registration Authorities of B-Trust and the verifiers of the Provider. The access to the personal data for the purpose of requesting its modification is carried out through the Provider or through the Registration Authorities of B-Trust at the addresses indicated on the Provider's website (www.b-trust.bg).

Certificate type:	
Period of validity:	
Public access allowed:	
Signatory	Personal data
ID document:	
First name:	
Middle name:	
Last name:	
	Address/ phone number/ e-mail
Region:	
City:	
Address:	
Postcode:	
Phone number:	
E-mail:	
	Certificate data
DN (Subject) of the request:	C=BG GN= SN= CN= serialNumber= emailAddress=

Provider:
Partner/ Relying Party

Signatory: