TERMS, PROCEDURE AND MODE

FOR THE USE OF
QUALIFIED ELECTRONIC SIGNATURE
AND
QUALIFIED TIME STAMP TOKEN

Version 2.1

July, 2017

History of changes to the document				
Version	**Author (s)**	**Date**	**Status**	**Comments**
2.1	Dimitar Nikolov	08.03.2017	Approved	Changes related to the implementation of Regulation 910/2014.

CONTENTS

List of terms and abbreviations

B-Trust®	Trade mark of the activity of “Borica” AD as Qualified Certificate Services Provider
CA	Certification Authority
CRL	Certificate Revocation List
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standards
ISO	International Standard Organization
OID	Object Identifier
OCSP	On-line Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivers-Shamir-Adelman
QSCD	Qualified Signature Creation Device
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
QTSA	Qualified Time Stamp Authority
QTST	Qualified Time Stamp Token
QCSP	Qualified Certification Services Provider
EDESA	Electronic Document and Electronic Signature Act
CRC	Communications Regulation Commission
LRA	Local Registration Authority
OACSP	Ordinance on the Activities of Certificate Service Providers
ORQESA	Ordinance on the Requirements for Qualified Electronic Signature Algorithms
CPS	Certificate Practice Statement of the QES Certificate Services Provider, Certificate Practice Statement of the Time Stamp Authority
CP	Certificate Policy of the QES Certificate Services Provider, Certificate Policy of the Time Stamp Authority
QES	Qualified Electronic Signature

Introduction

This document describes:

- The mode of use of the Qualified Electronic Signature (QES), for which the relevant qualified certificate has been issued to a Titular, as well as the mode of use of the Time Stamp Token issued by the QCSP “BORICA” AD;
- The terms and procedure for the use of QES, including the requirements for the treasure up of the Titular’s private key, and the terms and procedure for the use of the Qualified Time Stamp Token;
- Terms for the access to Qualified Certificate for QES and Qualified Time Stamp Token, as well as the method to verify the QES and the QTST.

Based on this document, each Titular of Qualified Certificate for QES and/or Trusting party of a QES and of a QTST will be able to define, to create and to follow a concrete Policy on signing/qualified verifying QES, as well as a Policy on the use of QTST.

I. TERMS, PROCEDURE AND MODE FOR THE USE OF QUALIFIED ELECTRONIC SIGNATURE

1. General rules on the use of the signature

1.1. Each Titular shall use QES in abiding by the following basic requirements:

- Strictly adhering to the EDESA, to the ordnances on its implementation and on the commonly established in the international practice recommendations and standards;
- Observing the highest level of treasure up/protection of the private key for electronic signature by the Titular;
- Adhering to the terms and procedures for generating the pair of keys in accordance with the B-Trust Certification Practice Statement and Certification Policy, regardless of whether the above-mentioned pair of keys is generated by the QCSP or by the Titular;
- Observing the terms for access to the private key – use of password/personal identification number (PIN);
- Strict compliance with the measures and procedures for identification and authentication of the applicant party for a Qualified Certificate for QES, according to the B-Trust Certification Practice Statement and Certification Policy;
- Impossibility of a subsequent use of QES in case of loss of smart-card (QSCD), in case of destruction of the private key for signing, after expired validity or termination of the relevant certificate;
- The publicly announced CPS, procedures and CP for the provision of certificate services by the QCSP;
- 24/7 public access to the Public Register of issued QES , to CRL, and to the service certificates of the QCSP through the Internet site;
- Observance of the guarantees and the insurance policy of the QCSP;
- Respecting of the non-property and property rights, in particular the intellectual property rights of the QCSP and the Titular.

2. Rules for signing

2.1. Before using the private key for signing an electronic document the Titular has to make sure that the corresponding certificate is for QES, i.e. the certificate is qualified and it is issued in accordance with the CP for this certificate, which meets the Titular needs;

2.2. It is recommended to check the CP by comparing with the identifiers, specified in the original copy of the B-Trust Certification Practice Statement and Certification Policy of the QCSP;

2.3. The CP on issuance and maintenance of the Qualified Certificate for QES is identified in the certificate with the following characteristics:

- Unique CP OID;

- Unique identifier for qualified certificate;
- Name of the QCSP;
- Date of issue and date of entry into force of the CP, which is a consequence of the date of issue and the date of entry into force of the B-Trust Certification Practice Statement and Certification Policy;
- Applicability to the specific type of the qualified certificate.

3. Way of use – trusted software applications

3.1. Signing with QES must always be performed with trusted software applications or with software applications certified under the LEG.

3.2. On the QCSP's website there is a published list with the trusted software applications suitable for the use of QES and for the relevant certificate, in accordance with its purpose;

3.3. It is in the due care of the Trusting party to check the purpose and the applicability of the Qualified Certificate for QES and the software applications used for the creation and verification of the signature.

3.4. The signing party, respectively the Trusting/verification party principally implements two ways for signing with QES and for verifying the signature:

- Local – a trusted software application for signing/verification will operate on a Author/Titular local system, with access to a local QSCD with QES. This way of working is used by the widely applicable and de-facto established as a standard local office applications for working with e-documents (MS Office, Adobe Acrobat, etc.) or client software packages and instruments for signing/verification provided by the QCSP;
- Remote – a trusted software application for signing/verification operates as a service or in a server system, with remote access to the QSCD with QES at the local system of the Author/Titular. QCSP provide online services for signing/verification.

4. Constrains on the use of the signature

4.1. QES has legal value of a handwritten signature, if used with an accompanying Qualified Certificate for QES, within the scope of this certificate, as well as, in terms of additionally agreed between the Titular and the Trusting party constrains on the way of use.

4.2. Constrains on the use of the signature in terms of value of the transactions, which the Titular may conduct with QES, and the statements that may be delivered by the Titular, are outside of the scope of the CP, under which the CA of the QCSP issues the relevant Qualified Certificate for QES. The restriction on the use of the issued certificates in respect to the value of the transactions, which the Titular may conduct with QES, is subject to agreement between the Titular and the Trusting party.

4.3. Constrains on the use of QES in terms of its purpose shall be recorded in the Qualified Certificate by the "Key Usage" and "Extended Key Usage" requisites.

4.4. The use of QES outside the recorded in the Qualified Certificate constrains shall not engage in any way the responsibility of the QCSP and is borne entirely by the

Titular or by the Trusting party. In this case, the QES accompanied by such a certificate will lose its legal value of a qualified signature.

5. Obligations of the Titular upon signing

5.1. Upon use of QES the Titular has to:

- Follow and comply strictly with the terms and procedures in the B-Trust Certification Practice Statement and Certification Policy, and the corresponding policies and practices for the use of the signature and the consumption of other certification services;
- Have a basic knowledge on the use of electronic signature and PKI technologies;
- Not to use the private key to create QES after the expiry of the certificate, or after suspension or termination of its validity;
- Notify each Trusting party on the due care taken in trusting QES and its accompanying qualified certificate.

6. Technical security and control

6.1. Detailed information on the requirements for treasure up the private key and on the creation of QES of a Titular is contained in the B-Trust Certification Practice Statement and Certification Policy of the QCSP.

7. Secrecy of the private key

7.1. In order to protect the secrecy of the private key the Titular has to:

- Ensure secure and trusted environment when using the pair of keys for the QES with a view to protect the secrecy of the private key;
- Use algorithms, according to the requirement of ORQESA;
- Notify immediately the QCSP in case of compromising or having suspicions for compromising the private key, by requesting simultaneous suspension or termination of the relevant certificate for the QES;
- Treasure up and protect reliably against loss and compromise the secrecy of his private key for the validity period of the certificate, according to the requirements set up in the B-Trust Certification Practice Statement and Certification Policy of the QCSP. Each use of the private key is considered as an action committed by the Titular;
- Change the initially provisioned PIN-code for access to the smart-card (private key) before using the QES, in case that the qualified certificate has been issued on a B-Trust smart-card.

8. Generation of new pair of keys

8.1. In view of reducing the risk from compromising the current pair of keys, the QCSP recommends that the Titular generate new pair of keys when renewing or reissuing certificate for QES.

9. Compromising the private key

9.1. According to the B-Trust Certification Practice Statement and Certification Policy of the QCSP, in case of compromising the Titular's private key, the latter shall

immediately notify the QCSP for initiating a procedure on termination of the Qualified Certificate for QES.

10. Destroying the private key

10.1. The Titular can destroy the private key by:

- Iinitializing ("deleting") the smart-card if the key is stored on a smart-card;
- Physical destruction of the media (smart-card).

11. Activation and deactivation of a private key

11.1. Upon initialization of B-Trust QSCD the following access codes are generated, and are provided to the Titular: code to unblock the QSCD “Unblock PIN” and initial user access code „User PIN”.

11.2. The Titular is obliged to change the „User PIN”, through the software provisioned with the B-Trust QSCD.

11.3. The QCSP recommends that the Titular periodically change the user access code QSCD.

11.4. The Titular shall duly treasure up and shall use only when necessary the provisioned code to unblock the B-Trust QSCD.

11.5. The access to the private key for creating QES is through entering the „User PIN” or by carrying out personal identification in any other way.

11.6. A private key for creating QES is deactivated by termination of the Qualified Certificate for QES.

11.7. If the private key has been saved on QSCD, the possibility of using it can be terminated by removing the smart card from the card reader.

11.8. If the private key has been saved on other media, the possibility of using it can be terminated by removing the media from the computer and suspending the access to the key file.

11.9. QSCD access codes are distributed to the Titular separately from the smart card.

II. ACCEPTANCE OF THE QUALIFIED ELECTRONIC SIGNATURE

1. Trust in the QES

1.1. The Trusting party - the addressee of an electronic statement or signed with QES electronic document of the Titular shall accept and trust, that the signature has legal value of a handwritten signature to the Trusting party and binds the Titular only after due care is taken to check all circumstances concerning the validity of the electronic signature.

2. Due care of the Trusting party

2.1. The use of QES implies that persons who trust the qualified certificate for the signature should have basic knowledge on the principles of operation of the B-Trust PKI Infrastructure of QCSP.

2.2. The Trusting party should take due care by:

- Trusting the certificate only in view of the purpose and terms of the CP, according to which the certificate has been issued and taking into account the additionally agreed and contracted with the Titular constrains for using the QES in Trusting party relations with the Titular;
- Checking the certificate for the indicated CP applicable to this certificate, and the purpose and constraints on the certificate validity;
- Checking the purpose of the signature in the fields: "Key Usage", "Extended Key Usage" and "Qualified Statement" of the certificate. The "Basic constrains" field has to be established as follows: “Subject Type = None”. The "Key Usage" field has to contain "Non-repudiation, Digital Signature". The "Qualified Statements" field has to contain the identifier ‘0.4.01862.1’;
- Checking the constrain on the use of the certificate with respect to the value of the property interest, if any. In the general case, the constrain is beyond the scope of the CP of the CSP for a qualified certificate for QES and is subject to concordance and agreement between the Author/Titular and the Trusting party. The constrain, if any, shall not refer to Provider’s responsibility for damages of the issued certificate for QES;
- Determining whether the certificate is not issued for test demonstration needs.

2.3. The Trusting party should make sure that the issued certificate is for QES. The verification shall be performed:

- On the basis of the recorded OID for the CP, under which the certificate has been issued by the QCSP;
- Based on the content in the field "Qualified Statements";

2.4. The Trusting party should check the format of the data that have been signed - to verify the electronic signature it is necessary to know exactly what information or object have been signed. The established international recommendations, standards and specifications for public key cryptography set the standard formats for QES to electronic statement or document of the Titular: PKCS # 7, CMS, XML-DSIG, XAdES, etc.

2.5. The Trusting party should verify that the QCSP is registered in the published Register of the CRC under the EDESA.

2.6. The Trusting party should make sure that the person entered on the certificate acts within his/her representative authority in respect to the Titular, if such registered.

2.7. The Trusting party should verify the status of the qualified certificate in the Public Register supported by the QCSP. The verification of the authenticity and integrity of the certificate – i.e. the signature of the QCSP does not provide verification of

its validity and all the damages occurred from the actions undertaken after completion of only such verification shall be borne by the Trusting party.

2.8. The Trusting party should verify by checking to an acceptable level of trust such as: operational certificate by the QCSP whether the certificate of the Titular has not been terminated or suspended. The termination or suspension of the certificate as a legal consequence leads to the invalidity of the signature. Validation status is carried out by using CRL, OCSP, or review of the Register of issued qualified certificates of the QCSP.

2.9. The Trusting party should check/verify the QES for electronically signed statements, and verify the electronic signature of the QCSP through the chain of certificates up to an acceptable level or to the root certificate. This verification has to be based on the X.509 standard. The validation check of the QES is regarding the successful confirmation of the validity of the certificates throughout the whole chain, in which the Qualified Certificate for QES participates. Particularly for the B-Trust domain, in this chain are involved the root certificate and the operational certificate of the QCSP.

2.10. The Trusting party should make sure that the applications, with which the Qualified Certificate for QES is used, are functionally applicable for the purpose the certificate has been issued, as well as in view to the security level specified in the respective CP.

2.11. The Trusting party has to make sure that such acceptance is reasonable under relevant circumstances. In the event that the circumstances require the need for additional guarantees for trust and confidence, the Trusting party should take due care for building full trust and confidence.

2.12. It is in the Trusting party due care taken to use a mechanism for a Qualified QES validation, which will ensure that:

- The public key, which is used for the actual check of the signature corresponds to what is displayed on the screen;
- The verification of using the private key is reliably confirmed and the verification results are displayed correctly;
- The Trusting party may determine if necessary the contents of the signed electronic document;
- The authenticity and validity of the certificate at the time of signing/use of QES are reliably verified;
- The results from the verification and Titular data are properly visualized;
- Any changes relevant to the security are identifiable.

2.13. The QCSP shall not be responsible for any damages to the Trusting party derived from failure to take the due care.

III. TERMS, PROCEDURE AND MODE OF USE OF THE QUALIFIED TIME STAMP TOKEN (QTST)

1. General rules

1.1. The CP of the specialized authority of the QCSP for QTST contains the terms and procedures for the issuance, delivery and maintenance of QTST for the users.

1.2. The QCSP issues QTST to any interested party by respecting a standard level of service.

1.3. User who needs a guaranteed service level of the QTST should conclude a contract with the QCSP.

1.4. The QCSP issues QTST with two types of content – for QES and for any electronic document.

1.5. The QTST has to be published in the Public Register of QTST to the specialized QTSA of QCSP.

2. Issuing QTST

2.1. The QCSP issues QTST under the common CP with an identifier „OID = 0.4.0.2023.1.1".

2.2. QTSTs with CP identifier different from the above-described are issued to users, who have a contract with the QCSP for Service Level Agreement (SLA) for the QTST.

3. Mode of use of QTST

3.1. QTST with Policy identifier „OID = 0.4.0.2023.1.1" are applicable for use in applications with different profile:

- Use of the QES at a specific point in time – the QTST is integrated to the QES of the signed document. This use of QTST creates "non-repudiation" of the QES over the time - i.e. the validity of QES extends beyond the period of validity of the Qualified Certificate for this QES. This mode of use of QTST enables the use of extended format of QES (XAdES, CAdES, PAdES) in the corresponding applications;
- Creating a QTST with content of an electronic document before a certain point in time, i.e. a certificate of irreversible content of the electronic document after the moment of the QTST. This mode of use of QTST is applied in building of archives, registers, e-forms, etc.

3.2. QTST with coordinated CP of issuance and use shall be used on specialized applications for the QTST users.

4. Constrain on the use of QTST

4.1. The CP of the QCSP with common identifier „OID = 0.4.0.2023.1.1" in the QTST itself shall not constrain the applicability of the provided QTST, at the discretion of users.

4.2. QTSTs with coordinated CP of issuance and use, included in these QTSTs shall only serve the specific parties, under the terms of the contract with the QCSP.

The QCSP shall not be responsible when the applicability of the QTST is beyond the specified CP.

5. Obligations of the parties in the use of QTST

5.1. The obligations and responsibilities of the QCSP for the provision and maintenance of QTST with common CP identifier "OID = 0.4.0.2023.1.1" are described in the document “Certificate Policy and Certificate Practice Statement of the Authentication B-Trust Time Stamp Authority” of the QCSP.

5.2. The obligations and responsibilities of the QCSP for the provision and maintenance of QTST with coordinated CP identifier shall be described in separate document Service Level Agreement (SLA), which is integral part of the contract with the QCSP.

5.3. The QTST users have to:

- Accept the root certificate of the QCSP, thus building the confidence to this QCSP and its specialized QTSA;
- Use the qualified certificate of the QTSA for the purpose to verify the QES in the QTST;
- Carry out verifications of QES by following the instructions in this document.

5.4. The Trusting party should verify the QES in the QTST and the validity of the certificate of the QTSA.

5.5. In the event that the certificate has expired the Trusting party should:

- Check in the CRL for this certificate;
- Verify the security level of the used Secure Hash Algorithm according to the CP;
- Check the security level of the algorithms and the length of the key pair of the QES.

6. Technical security and control

6.1. The technical security and control with the use of QTST are in full compliance with the public document “Certificate Policy and Certificate Practice Statement of the Authentication B-Trust Time Stamp Authority” of the QCSP.

IV. ACCEPTANCE OF THE QUALIFIED TIME STAMP TOKEN

1. Trust in the QTST

1.1. The Trusting party - addressee in the use of QTST should trust and accept, that the QTST has official certification power to it and binds the QCSP, only after due care is taken to verify all the circumstances concerning their validity of the issued QTST.

2. Due care of the Trusting party

2.1. The Trusting party should check in the Public Register for a QTST of the QCSP by its number.

2.2. The Trusting party should take due care by following the instructions mentioned and described in this document.