CERTIFICATE POLICY

FOR THE ISSUANCE OF QUALIFIED ELECTRONIC SEAL AND WEBSITE AUTHENTICATION CERTIFICATES TO PAYMENT SERVICE PROVIDERS UNDER PSD2

(B-Trust QCP-PSD2 QSealC and QWAC)

Version 2.0

March 1, 2020

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	01.04.2019	Approved	Initial release
2.0	Dimitar Nikolov	01.03.2020	Approved	Technical corrections

CONTENTS

TERMS AND ACRONYMS

QTSP	Qualified Trust Service Provider
EGN	A uniform civil number assigned to each Bulgarian citizen or resident foreign national
ES	Electronic Signature
ESeal	Electronic Seal
ESeal PSD2	Electronic Seal for PSD2
EDECSA	Electronic Document and Electronic Certification Services Act
QES	Qualified Electronic Signature
QC	Qualified Certificate
QTS	Qualified Trust Services
QSealC PSD2	Qualified Certificates for Electronic Seal for PSD2
QWAC PSD2	Qualified Certificate for Website Authentication for PSD2
CRC	Communications Regulation Commission
LRA	Local Registration Authority
PIN	Personal Identification Number
Practice Statement	Practice Statement for providing QC and Qualified Trust Services
Policy	Policy for providing QC and Qualified Trust Services
Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
RA	Registration Authority
Website	A collection of related web pages, including multimedia content, typically identified with a common domain name (DN), and published on at least one web server
CA	Certification Authority
eSeal PSD2	Electronic Seal for PSD2
BG	Bulgaria
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CENELEC	European Committee for Electrotechnical Standardization
CP	Certificate Policy

CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
IP	Internet Protocol
OID	Object Identifier
OCSP	On-line Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QC	Qualified Certificate
QSCD	Qualified Signature Creation Device
RQSCD	Server component in the cloud QES platform of B-Trust for secure remote signature creation
RA	Registration Authority
RSA	Rivest – Shamir - Adelman / encryption algorithm used for creating a signature
SCT	Signature Creation Token / software token (PKCS#12 crypto file)
B-Trust SCT	PKCS#12 / crypto file (software token)
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
URL	Uniform Resource Locator
QCP-l	Certificate policy for EU qualified certificates issued to legal persons
QCP-w	Qualified certificate policy for EU qualified website authentication certificates

PSD2 RELATED ACRONYMS

PSD2	Payment Service Directive 2
PSU	Payment Service User
PSP	Payment Service Provider
PIS	Payment Initiation Service

PISP	Payment Initiation Service Provider
AIS	Account Information Service
AISP	Account Information Service Provider
PIIS	Payment Instruments Issuer Service
PIISP	Payment Instruments Issuer Service Provider
ASPSP	Account Servicing Payment Service Provider
TPP	Third Party Payment Service Provider (PISP, AISP or PIISP)
RTS	Regulatory Technical Standard
EBA	European Banking Authority
CA	Competent Authority
TPP	Trusted Payment Provider – ASPSP, PISP, AISP or PIISP

SCOPE AND APPLICABILITY

The present document:

- Has been drawn up by BORICA AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- Is effective as of 01.04.2019;
- Is titled “Policy for Providing Qualified Electronic Seal and Website Authentication Certificates to Payment Service Providers in Compliance with PSD2 (B-Trust QCP-PSD2 QCSealC and QWAC)“;
- Is associated with the published current version of the document „Certification Practice Statement for qualified certificates and qualified certification services (B-Trust CPS-eIDAS)”, which contains the general terms and conditions for the procedures of identification, QC issuance and maintenance, and the security level requirements for generating and storing the private key for these certificates;
- Has been developed in accordance with the formal requirements for content, structure and scope, as set out in the international guideline RFC 3647, including sections with additional information that are specific and applicable to PSD2 qualified certificates according to ETSI TS 119 495 V1.1.2 and COMMISSION DELEGATED REGULATION (EU) 2018/389, prepared on the basis of Regulatory Technical Standards (RTS), submitted by the European Banking Authority (EBA), in accordance with Art. 98 of PSD2;
- Is based on the current versions of the documents “Qualified Certificate Policy for providing qualified certificates for electronic signature/seal (B-Trust QCP-eIDAS QES/QESeal)” and „Qualified Certificate Policy for providing qualified certificates for website authentication (B-Trust QCP-eIDAS Web SSL/TLS)” and determines the Policy of the QTSP on qualified PSD2 certificates;
- Has the nature of general terms within the meaning of Art. 16 of the Obligations and Contracts Act. These conditions are part of the Certification Service Agreement concluded between the Provider and Users under Art. 23 of the EDECSA. The Agreement may contain special conditions that shall have priority over the general terms in this document.
- Is a public document with the purpose to establish the conformity of the activity of the Provider BORICA AD with the EDECSA and the legal framework, and the specific requirements of ETSI TS 119 495 V1.3.1 and COMMISSION DELEGATED REGULATION (EU) 2018/389 to PSD2;
- is publicly available anytime on the Provider's website: https://www.b-trust.bg/documents;
- May be amended by BORICA and each new revision of this document shall be published on the Provider's website.

The present document has been prepared in accordance with:

- Electronic Document and Electronic Certification Services Act (EDECSA);
- Ordinance on Liability and Termination of Activities of Trust Service Providers;
- Ordinance on the requirements to the algorithms of creation and verification of qualified electronic signature;
- Regulation (EU) № 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Directive (EU) 2015/2366 of the European Parliament and of the Council;

- Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication;
- Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) – Final Report EBA/RTS/2017/02.

The contents and structure of this document is based on information contained in the following ratified international recommendations, specifications and standards:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816: ESSCertIDv2 Update for RFC 3161;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 412-1,2,3 и 5: Certificate Profiles;
- ETSI TS 119 495 V1.3.1 Qualified Certificate Profiles and TSP Policy Requirements under the Payment Services Directive (EU) 2015/2366;
- CA/Browser Forum: Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, v. 1.4.1.

Any information related to the present document may be obtained from the Provider:

BORICA AD
41 Tsar Boris III Blvd.
1612 Sofia
Bulgaria
Tel: +359 0700 199 10
E-mail: info@b-trust.org
Web: www.b-trust.bg

1 OVERVIEW

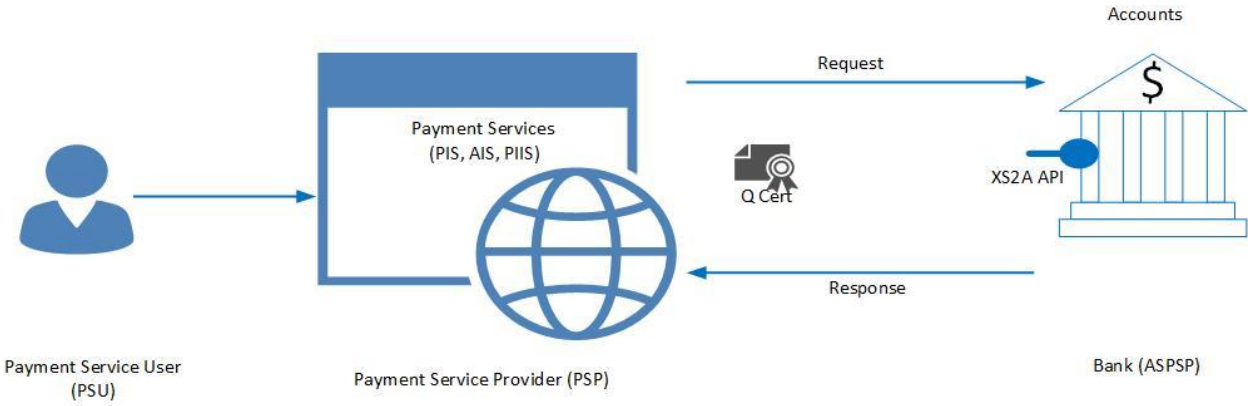
1.1 PSD2 PAYMENT SERVICES AND PARTICIPANTS

The European Commission has published a new directive on payment services in the internal market (PSD2). Member States have to adopt this directive into their national law until 13th of January 2018.

PSD2 contains regulations of new services to be operated by so called third party payment service provider (TPP) on behalf of a payment service user (PSU). These new services are:

- payment initiation service (PIS) to be operated by a Payment Initiation Service Provider (PISP) as defined by article 66 of PSD2;
- account information service (AIS) to be operated by an Account Information Service Provider (AISP) as defined by article 67 of PSD2, and
- service for confirmation of the availability of funds necessary for execution of card based payment transaction as defined by article 65 of PSD2; the service is provided by Payment Instrument Issuer Payment Service Provider (PIISP) towards Account Servicing Payment Service Provider (ASPSP).

According to PSD2 a PSP (PISP, AISP, PIISP) shall identify itself every time it accesses an account using the XS2A interface provided by an ASPSP. Article 29 of EBA RTS 2017 substantiates this by requiring that this identification shall rely on qualified certificates according to the Regulation 910/2014 (eIDAS).



The Qualified Certificates are issued by a Qualified Trust Service Provider (QTSP). Supervision and qualification of the QTSP are regulated by Regulation 910/2014.

BORICA as a QTSP under the Regulation (eIDAS) issues qualified certificates to PSPs for their identification at the XS2A interface.

PSD2 and EBA RTS require QTSPs (in particular, BORICA) to apply additional requirements for identification when requesting the issuance and revocation/suspension of PSP certificates.

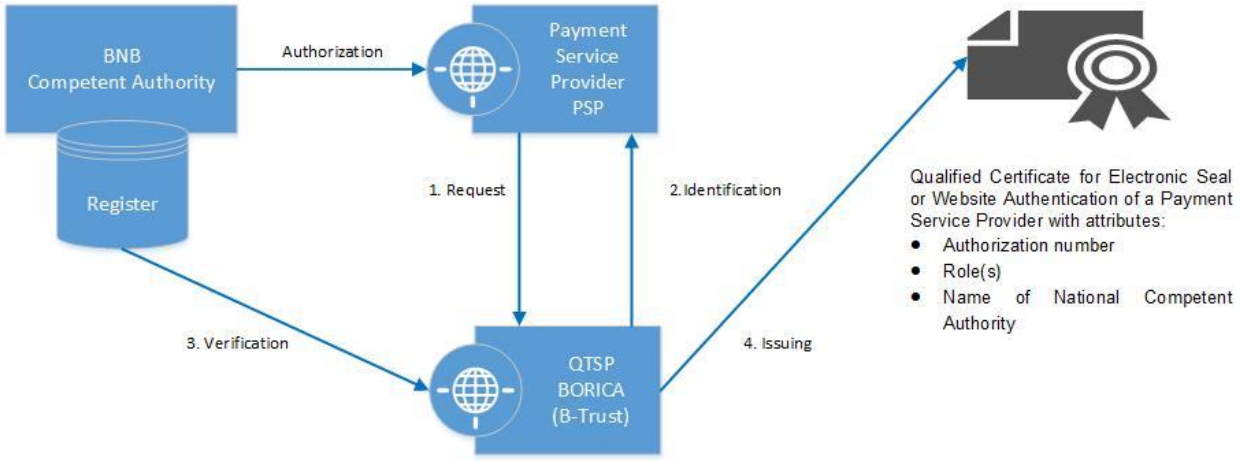
A qualified certificate is issued to a PSP only if authorized by the national competent authority under PSD2 – the BNB, to offer the new payment services as a TPP. On the other hand, a PSP

certificate is revoked only if the authorization of the PSP is withdrawn by the national competent authority, the BNB.

In addition article 29 of EBA RTS defines some special attributes to be included into the qualified certificate of the PSP:

- PSP Authorization Number;
- Role of the PSP, which can be:
  - Payment Initiation Service Provider
  - Account Information Service Provider
  - Payment Instrument Issuer Payment Service Provider
  - Account Servicing (payment service provider)
- Name of the national competent authority - the BNB, registered the PSP.

The values of these attributes are determined by the national competent authority, the BNB, as part of the authorization or issuance of license to the PSP.
BORICA as a QTSP issuing qualified certificates to PSP has to verify the correctness of these attributes as part of the identification of the PSP before issuing the certificate (step1 - request, step 2 – identification, step3 – attributes verification, and step 4 – issuing certificate).



The present document defines specific additions to the current certificate policies of BORICA for the respective qualified certificates, necessary to comply with the requirements for issuing and revocation of the qualified certificates to PSPs, defined by PSD2 and EBA/RTS/2017.

The Policy under this document has to be implemented within18 months after the adoption of the official version of EBA/RTS (2017).

1.2 PKI PARTICIPANTS AND QUALIFIED CERTIFICATES

According to article 29 of EBA RTS the identification of PSP shall rely on qualified certificates for electronic seals or for website authentication as defined by (30) respectively (39) of article 3 of the Regulation (eIDAS 2014), without specifying by whom or by which circumstances it has to be decided whether qualified certificates for electronic seals or for website authentication have to be used. Nevertheless these certificates should always be used only for a purpose intended by the Regulation eIDAS, i.e.:

- A qualified certificate for electronic seal shall be used if the integrity and origin of data shall be proved (article 35 2. of the Regulation) - to ensure the integrity and origin of the PSU account data between the parties and to initiate the payment:

- A qualified certificate for website authentication shall be used to authenticate a domain, which domain name has to be part of the certificate (article 45 and annex IV (e) of the Regulation) - in mutual (bilateral) identification and authentication in the process of establishing a secure communication channel (TLS) between the parties:

For both types of Qualified Certificates, the specific requirements and additional special attributes for purposes of PSD2 shall remain valid.

The qualified PSD2 certificates issued and maintained by BORICA according to this Policy address the following PKI participants:

- BORICA as a QTSP issuing/maintaining the certificates,
- PSP (PISP, AISP, PIISP) using the certificates, and
- ASPSP - as relying parties.

BORICA issues qualified certificates to PSP (AISP, PISP and PIISP). In addition it provides a service for suspension/revocation of certificates and for verification of their validity using CRL or Online Certificate Status Protocol (OCSP). For its part, a PSP uses its certificate to identify itself at the XS2A interface as required by PSD2 (articles 65, 66 and 67) and EBA RTS (article 27 and 29), and to sign its requests using the corresponding private key and including its certificate into the request message.

An ASPSP is participating as relying party. The ASPSP is verifying the electronic signature and the certificate, which are part of an incoming request message at the XS2A interface provided by the ASPSP according to article 27 of EBA/RTS. The ASPSP has to determine, based on its own risk analysis and management, the detailed steps to be performed for the verification of the PSP certificates - check against a “white list” of certificates managed by the ASPSP, check against a

CRL or online requests at an OCSP of B-Trust provided by BORICA, check of the national trusted list containing the certificates of all QTSPs in the country (as a trust basis).

Figure 1 shows the relationship between the PKI participants when using the qualified certificates in PSD2 services.

To enhance the XS2A interface (bilateral strict authentication of the participants) the ASPSP also identifies itself at the XS2A interface. In this case BORICA shall issue qualified certificates required by EBA/RTS and PSD2 also to ASPSP. ASPSP will sign/seal its messages (responses) to a PSP using the corresponding private key and will include its certificate into the messages sent to the PSP and the PSP will be the relying party.

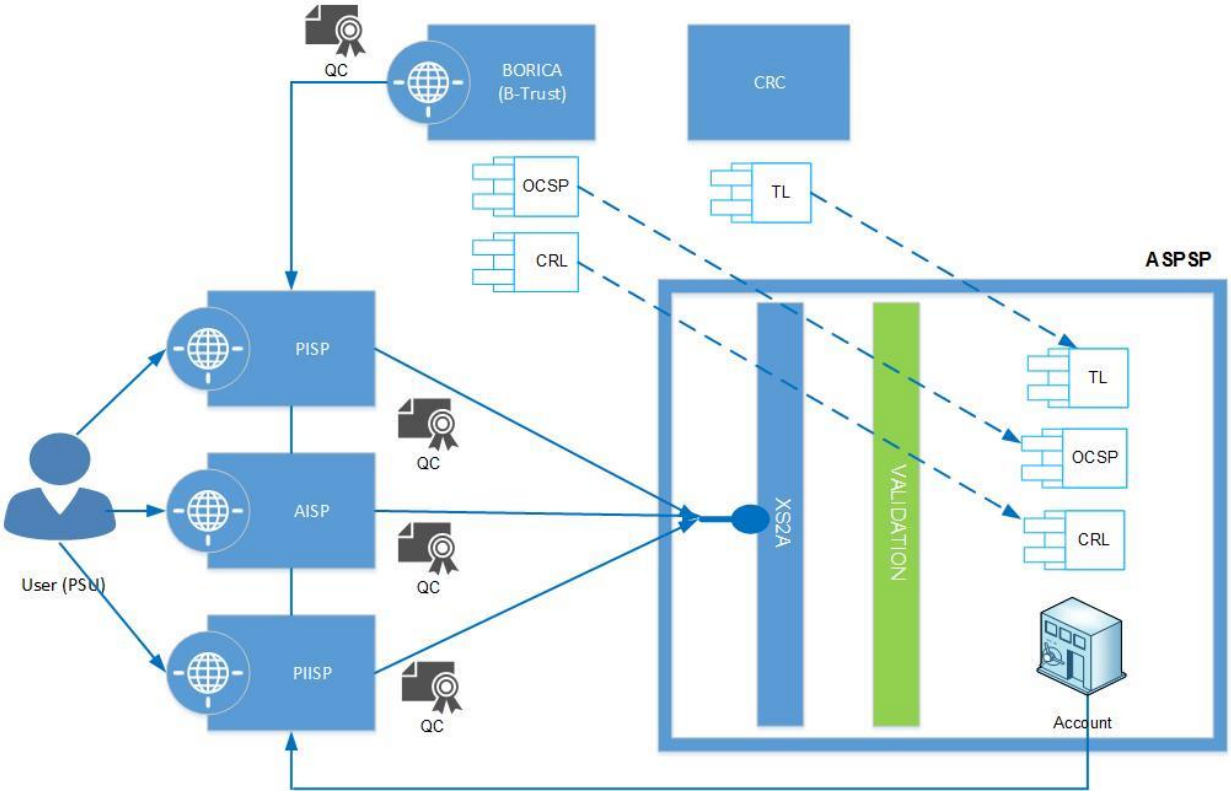


Figure 1. PKI participants in the PSD2 payment services

1.3 SUPERVISION OF THE PKI PARTICIPANTS IN PSD2

The Policy of issuing Qualified Certificates (for Website Authentication and Qualified Electronic Seal) with specific attributes according to this document takes into account the two areas of regulation and supervision for PKI participants in PSD2 services:

- For BORICA as a QTSP – the National Supervisory Body (the CRC) according to Regulation 910/2014 and the EDESCA;
- For the PSP - the National competent/supervisory authority (the BNB) according to PSD2, which authorizes the service providers, i.e. allows them to provide payment services under PSD2.

In this respect, these national competent authorities are also indirect participants in the implementation of this Qualified Certificate Policy.

By combining these two areas of regulation, the Policy under this document sets out the conditions under which BORICA as a QTSP issues qualified certificates for payment services.

Figure 2 presents the relations to supervision of the PKI participants under this Policy from the point of view of the PSP (being a payment institution).

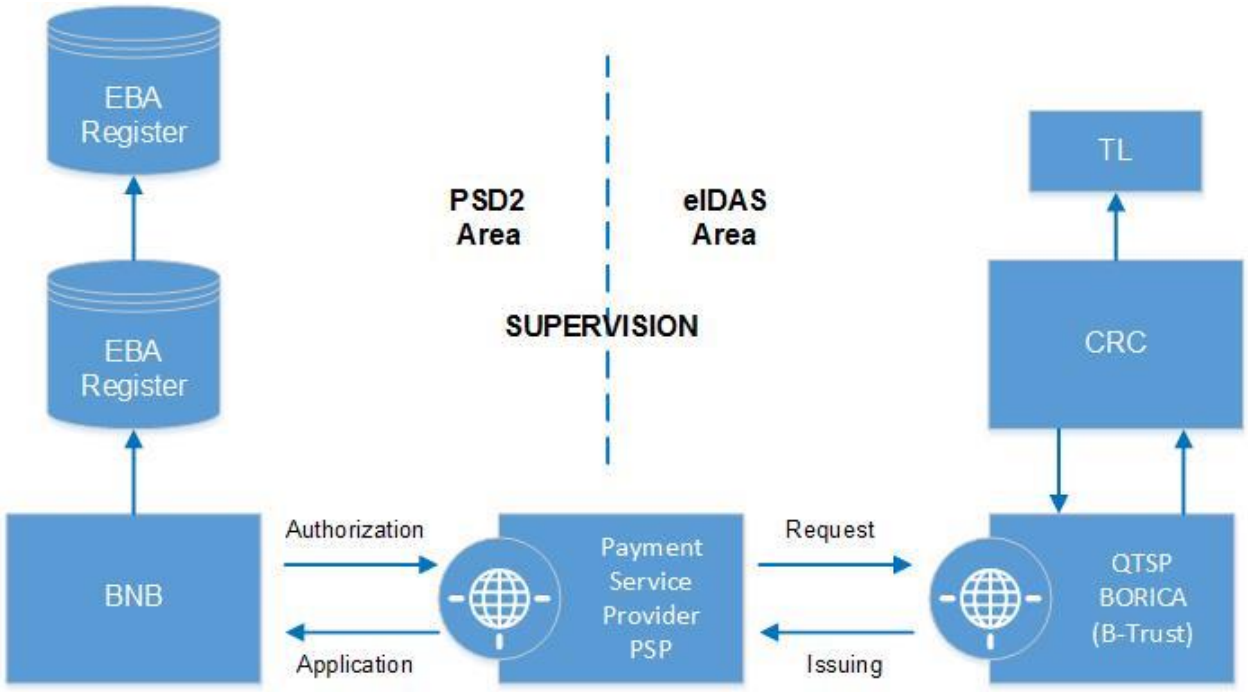


Figure 2. PKI participants in the PSD2 payment services – supervision (regulation)

2 INTRODUCTION

This Policy:

- Refers only to the qualified certificates for qualified electronic seal and website authentication, issued by BORICA in compliance with RTS/EBA for PSD2 and Regulation (EU) № 910/2014 and the applicable legislation of the Republic of Bulgaria;
- Defines the specific conditions and requirements that the QTSP implements when issuing and maintaining these qualified certificates, and their applicability with respect to security level and restrictions in their use;
- Defines the technical profiles and content of the qualified certificates for electronic seal and website authentication for participants in the PSD2 payment services;
- Is implemented through common technical procedures and meets the security requirements for generating and storing the private key corresponding to a public key in the certificates specified in the Certification Practice Statement of the QTSP;

- Determines the applicability and the level of trust in the certified facts in the qualified certificates for electronic seal and website authentication.

It is assumed that a Payment Service Provider who uses this document has the knowledge and understanding of public key infrastructure (PKI), certificates and the concept of electronic signature/seal. Otherwise it is recommended to get acquainted with these concepts and with the document „Certification Practice Statement for qualified certificates and qualified certification services" of BORICA (B-Trust CPS-eIDAS) before using this document. In any case, this document should be used together with the Certification Practice Statement of BORICA.

B-Trust® public key (PKI) infrastructure of BORICA is built and functions in compliance with the legal framework of Regulation 910/2014, and the EDECSA, and with the international specifications and standards ETSI EN 319 411-1/5 and ETSI EN 319 412.

BORICA uses OIDs in the B-Trust PKI infrastructure, formed on the basis of code 15862, assigned to BORICA by IANA in the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA Registered Private Enterprise) and in accordance with ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).

BORICA has informed the CRC about the start of activity as a QTSP under the Regulation 910/2014, the EDECSA and current legislation. The QTSP notifies the Users of its accreditation for providing the QCs specified in this document.

The accreditation of BORICA as a QTSP under the Regulation and the EDECSA aims to achieve the highest security level of the QCs provided according to this Policy and better synchronization of these activities with similar activities provided in other Member States of the European Union.

In regard to relations with Users and third parties, only the current version of the Policy at the time of using QCs for qualified electronic signature/seal issued by BORICA is valid.

3 GENERAL CHARACTERISTICS OF THE CERTIFICATES

Pursuant to this Policy, BORICA as a QTSP issues and maintains the following types of qualified certificates for Payment Service Providers under PSD2:

- **QSealC PSD2 –** Qualified Electronic Seal Certificate (of a payment institution) for PSD2;
- **QWAC PSD2 –** Qualified Website Authentication Certificate (of a payment institution) for PSD2.

These certificates have the status of qualified certificates within the meaning of Regulation 910/2014.

3.1 QSEALC PSD2 – GENERAL CHARACTERISTICS

1. The Qualified Electronic Seal Certificate PSD2 issued under this Policy has the status of a qualified certificate within the meaning of the Regulation 910/2014 and of the EDECSA.
2. QSealC PSD2 is issued only to a legal person – Payment Service Provider under PSD2 who is the creator of the seal, and serves to authenticate the Service Provider and his relation with

his public key and to ensure the integrity and origin of the data in his electronic statements/messages.

3. For issuing this certificate, the personal presence of the PSP representative is required at the RA/LRA of BORICA for verification of the identity of the legal person of the PSP and the identity of its authorized person.
4. The identification procedure at the RA/LRA includes evidence of the identity and the authorization of the PSP and their verification under the order of sections 6.1 - 6.6 of this document.
5. The verification of the request for issuing QSealC PSD2 is done in the order of the above items and provides the highest level of security regarding the PSP identity and his relation with the provided public key.
6. The request for QSealC PSD2 may also include the natural person authorized to represent the PSP. The identity of the natural person is also verified.
7. A PSP can generate itself the key pair using approved by the Provider or other licensed software with an equivalent security level that is compatible with the B-Trust infrastructure.
8. (Option) It is acceptable for the Payment Service Provider to use a hardware token compatible with the B-Trust infrastructure to generate and store the key pair for QSealC PSD2. The PSP generates the key pair using B-Trust QSCD and the relevant software or other equivalent QSCD that is compatible with the Provider's infrastructure.
9. The private key for creating a QSealC PSD2 is generated using the approved or licensed software and can be stored in a portable software cryptographic file (PKCS # 12) and transferred to systems of the Payment Service Provider.
10. When the key pair is generated at the Provider, the issued QSealC PSD2 of the PSP certifying a public key corresponding to the private key is recorded to a portable software cryptographic file (PKCS # 12) together with the official certificates of BORICA and is provided to the PSP.
11. When the key pair is generated at the PSP, it is within the responsibility of the PSP to create a portable software token.
12. QSealC PSD2 is not renewed. The Payment Service Provider may request from BORICA issuance of a new QSealC PSD2 with a new key pair.
13. BORICA reserves the right to add, if necessary, additional attributes to the QSealC PSD2.

3.2 QWAC PSD2 – GENERAL CHARACTERISTICS

1. The Qualified Website Authentication Certificate issued under this Policy has the status of a qualified certificate within the meaning of the Regulation 910/2014 and of the EDECSA if used for authentication during the process of setting up secure communication channel (TLS).
2. This certificate is issued to a Payment Service Provider and it authenticates the electronic identity and its accreditation with a high degree of certainty for the browser client that the website accessed is owned by the organization identified in the certificate.
3. For issuing this certificate, the personal presence of the PSP representative is required at the RA/LRA of BORICA for verification of the identity of the legal person of the PSP and the identity of its authorized person.

4. The identification procedure includes submission of evidence of ownership of the domain hosting the website of the PSP and evidence of its identity and that of the authorized person, and their verification.
5. The identification procedure at the RA/LRA includes evidence of identity and the authorization of the PSP, the identity of the authorized person and their verification under the order of sections 6.1 - 6.6 of this document.
6. The verification of the request for issuing QWAC PSD2 is done in the order of the above items and provides a high degree of certainty regarding the PSP identity and its relation with the provided public key.
7. Regarding the use of the TLS/SSL protocol, the policy for this certificate allows a sufficient level of security for the browser client accessing the website – the use of approved or licensed software for generating and cryptographic software token for storing the private key corresponding to the public key in the website authentication certificate.
8. A PSP can generate itself the key pair using approved by the Provider or other licensed software that is compatible with the B-Trust infrastructure.
9. The key pair of the website authentication certificate of the PSP is generated by software and the private key is stored in a portable software cryptographic file (PKCS # 12) that can be transferred to systems of the PSP.
10. When the key pair is generated at the Provider, the issued certificate is recorded to a portable software cryptographic file (PKCS # 12) together with the official certificates of BORICA and is provided to the PSP.
11. When the key pair is generated at the PSP, it is within responsibility of the PSP to create a portable software token.
12. QWAC PSD2 is not renewed. The Payment Service Provider may request from BORICA issuance of a new QWAC PSD2 with a new key pair.
13. BORICA reserves the right to add, if necessary, additional attributes to the QWAC PSD2.

3.3 ATTRIBUTES OF THE QUALIFIED CERTIFICATES REQUIRED BY PSD2 (RTS)

The qualified certificates issued to Payment Service Providers contain attributes with specific data, required by the PSD2 (RTS).
The specific attributes of PSD2 are included and encoded in the Qualified Certificate as follows:

- in *QCStatement* of the qcStatements extension as specified in clause 5.1 of ETSI TS 119 495;
- in *organizationIdentifier* attribute of the Subject Distinguished Name field as specified in clause 5.2.1 of ETSI TS 119 495.

The *QCStatement* contains the following attributes of qualified certificate for PSD2, as required in article 34 of RTS:

- role of the PSP (*rolesofPSP*), which may be one or more of the following:
  - Account servicing (*PSP_AS*);
  - Payment initiation (*PSP_PI*);
  - Account information (*PSP_AI*);
  - Issuing of card-based payment instrument (*PSP_IC*).
- name of the national competent authority where the PSP is registered – full name (*NCAName*) or the unique identifier (*NCAId*).

The *organizationIdentifie*r attribute of the Subject Distinguished Name field contains the Authorization number of the Payment Service Provider, provided by the National Competent Authority (the BNB), maintaining a Public Register of Payment Service Providers in the Country.

3.4 POLICY IDENTIFIERS

3.4.1 QSealC PSD2 – identification of Policy and qcStatements extension of the certificate

1. BORICA as a QTSP applies and supports common policy identified in the QSealC of a legal person with a current policy identifier OID= 1.3.6.1.4.1.15862.1.7.1.7, which corresponds to the policy „qcp-l" (OID 0.4.0.194112.1.1) based on ETSI EN 319 411-2.
2. The QTSP additionally enters the policy „qcp-public" (O.I.D. = 0.4.0.1456.1.2) based on ETSI EN 101 456 in the QSealC, indicating that the private key has not been generated and is not stored and used on a QSCD.
3. The QTSP enters an identifier „id-etsi-qcs-QcCompliance" (OID=0.4.0.1862.1.1) in the „Qualified Statements" attribute of the QSealC, indicating that the certificate is qualified.
4. The QTSP enters an identifier „id-etsi-qcs-QcType" (OID=0.4.0.1862.1.6) with the value „id-etsi-qct-eseal" (oid=0.4.0.1862.1.6.2) in the „Qualified Statements" attribute of the QSealC, indicating that the certificate is used for qualified electronic seal.
5. The QTSP enters an identifier „id-etsi-qcs-QcPDS" (OID=0.4.0.1862.1.5) in the „Qualified Statements" attribute, with a value indicating the address (URL-link), on which the B-Trust PSD2 Disclosure Statement of the QTSP has been published.
6. The QTSP includes in the QSealC, the "Qualified Statements" field, attributes with data required by RTS (PSD2) according to section 3.3 of this document.

3.4.2 QWAC PSD2 – identification of Policy and qcStatements extension of the certificate

1. BORICA as a QTSP applies and supports common policy identified in the QWAC with a current policy identifier OID=1.3.6.1.4.1.15862.1.7.1.8, which corresponds to the policy "OVC" (OID = 0.4.0.2042.1.7) based on ETSI TS 319 411-1.
2. The QTSP enters in the „Certificate policy" attribute of the certificate a policy with OID = 2.23.140.1.2.2, corresponding to CA/B Forum SSL OV (PSP is a legal person).
3. The QTSP enters in the „Certificate policy" attribute of the certificate a policy with OID = 0.4.0.19495.3.1, corresponding to EU PSD2 QWAC Certificate policy (QCP-w-psd2) according to ETSI TS 119 495 v.1.3.1.
4. The QTSP includes an identifier „id-etsi-qcs-QcCompliance" (OID=0.4.0.1862.1.1) in the „Qualified Statements" attribute of certificate, indicating that the certificate is qualified.

5. The QTSP includes an identifier id-etsi-qcs-QcType (0.4.0.1862.1.6) = 0.4.0.1862.1.6.3 (id-etsi-qct-web) in the „Qualified Statements" attribute of the certificate indicating that the certificate is for website.
6. The QTSP includes an identifier „id-etsi-qcs-QcPDS“ (OID=0.4.0.1862.1.5) in the „Qualified Statements" attribute, with a value indicating the address (URL-link), on which the B-Trust PSD2 Disclosure Statement of the QTSP has been published.
7. The QTSP includes in the QSealC, the “Qualified Statements” field, attributes with data required by RTS (PSD2) according to section 3.3 of this document.

3.5 PURPOSE AND USAGE

3.5.1 QSealC PSD2

1. A Payment Service Provider uses QSealC PSD2 for placing electronic seal as a Creator (according to Regulation 910/2014) on electronic documents and data in electronic payment transactions/applications which require the highest level of information security.
2. In accordance with the Regulation 910/2014 QSealC PSD2 should not be used and applied as an electronic signature of a legal person.
3. QSealC PSD2 serves only to authenticate the source and integrity of sealed electronic documents/statements. When a transaction requires a qualified electronic signature of the legal person of the PSP, the qualified electronic signature of an authorized representative of the PSP is accepted as equivalent.
4. The due diligence of the Relying Party in the electronic payment transaction is to verify the purpose and applicability of the certificate and the software applications, with which the seal is created and verified, when trusting the electronic seal accompanied by this certificate.
5. Before trusting the electronic seal, the Relying Party should check in the profile of QSealC PSD2 (section 4.1 of this document) the policy indication applicable to this certificate (Certificate Policy attribute), and the PSD2 specific attributes in the psd2-qcSatement of the "qc Statements" extension, as well as the limitations of the certificate described in the “Key Usage” and “Extended Key Usage” attributes.
6. The validity of the QSealC PSD2 issued to PSP is 1 (one) or 3 (three) years. The certificate cannot be renewed. The provider shall issue a new QSealC PSD2.

3.5.2 QWAC PSD2

1. The PSP uses QWAC PSD2 to identify its domain and its accreditation with an adequate level of certainty for the browser client that the website he is accessing is property of the person identified in the certificate.

2. The PSP uses QWAC PSD2 in mutual (bilateral) identification and authentication during the process of establishing a secure communication channel (TLS) between the parties.
3. The QWAC PSD2 of a PSP has the status of a qualified certificate only regarding the authentication of the PSP identified by it.
4. The due diligence of the Relying Party in the electronic payment transaction is to verify the purpose and applicability of the certificate and the software applications, with which it is used.
5. Before trusting the website authenticity, the Relying Party should check in the profile of QWAC PSD2 (section 4.2 of this document) the policy indication applicable to this certificate (Certificate Policy attribute), and the PSD2 specific data in the psd2-qcSatement of the "qc Statements" extension, as well as the limitations of the certificate described in the “Key Usage” and “Extended Key Usage” attributes.
6. The validity of the QWAC PSD2 is 825 days. The certificate cannot be renewed. The provider shall issue a new QWAC PSD2 (to a PSP).

3.6 USE OF CERTIFICATES OUTSIDE THE FIELD OF APPLICATION AND RESTRICTIONS

When a User of a payment service or a Relying party use or trust QSealC PSD2 and QWAC PSD2 with a purpose other than those specified in the “SubjectAlternativeName”, "Key Usage", "Extended Key Usage," "Certificate Policy," or "Qualified Statements" requisites, the responsibility is entirely theirs and does not engage BORICA as a QTSP in any way.

3.7 POLICY ADMINISTRATION

1. This Certificate Policy is subject to administrative management and supervision by the Board of Directors of BORICA AD.
2. Changes, modifications and additions are admissible, which do not affect the rights and obligations arising from this document and the standard service agreement between the Provider and Users/Relying parties after approval and validation by the Board of Directors.
3. The location and content of the PSD2 attributes may change according to the update of the relevant legislation/standards while ensuring that such change does not conflict with the mandatory profile of a Qualified Electronic Seal and Website Authentication Certificates issued to legal entities.
4. Each submitted and approved new version of this document shall be immediately published on the website of the Provider.
5. Any comments, inquiries and clarifications regarding this document may be addressed to:
   - E-mail address of the Certification Authority: info@b-trust.org ;
   - E-mail address of the Provider: info@borica.bg ;
   - Tel.: 0700 199 10, fax: (02) 981 45 18.

4 CERTIFICATE PROFILES

4.1 QUALIFIED ELECTRONIC SEAL CERTIFICATE

Field/ Extension	Attributes	Value/Meaning
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Common name: Common name of the Payment Service Provider (legal person) by which he is known – may not exactly match the name in the attribute “O”]
	G =	[First name of the representative of the legal person of the PSP or an authorized person]
	SN =	[Surname name of the representative of the legal person of the PSP or an authorized person]
	SERIALNUMBER =	[Identifier of the representative of the legal person of the PSP or an authorized person. • For a Bulgarian citizen - one of the following: o PNOBG-XXXXXXXXXX for Personal ID o PASSBG-XXXXXXXX for passport number o IDCBG-XXXXXXXXX for ID card number o TINBG-XXXXXXXXX for tax number of a natural person o PI:BG-XXXXXXXXX for ID number of a foreign citizen o BT:BG-XXXXXXXXX for natural person number issued by B-Trust CA • For a foreign citizen – one of the following: o PNOYY- XXXXXXXXX for national identity number o PASSYY- XXXXXXXX for passport number o IDCYY- XXXXXXXXX for national ID card number where YY is the country code of the representative of the legal person of the PSP or an authorized person under ISO 3166]

	O =	[Name of the PSP (Organization of legal person)]
	2.5.4.97= (organizationIdentifier)	[Authorization number of the PSP, issued by the BNB (national competent authority) with the following structure: PSDBG-BNB-xxxxxxxxxx, where xxxxxxxxxx – number from the Public Register of Payment Services Providers maintained by the BNB]
	E =	[Email address]
	C =	BG or YY where YY is the code of the country under ISO 3166 where the Creator is registered
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[hash of „Public key "]
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer"]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.7 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.2 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.1
Enhanced Key Usage	-	Secure Email
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment
Qualified Statements	qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semantics-identifiers (oid=0.4.0.194121.1) / id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
	qcs-QcCompliance (qcStatement-1)	id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)

	qcs-QcType (qcStatement-6)	id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)	
	psd2-qcStatement (oid=0.4.0.19495.2)	PSD2QcType	rolesofPSP (0.4.0.19495.1) NCAName NCAId	One or more of the specified roles PSP_AS (0.4.0.19495.1.1) PSP_PI (0.4.0.19495.1.2) PSP_AI (0.4.0.19495.1.3) PSP_IC (0.4.0.19495.1.4) BNB (Bulgarian National Bank) (Name of national competent authority – BNB) PSDBG-BNB-xxxxxxxxxx (ID of national competent authority – BNB)
	qcs-QcPDS (qcStatement-5)	id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/psd2_pds_en.pdf language=en	

4.2 QUALIFIED WEBSITE AUTHENTICATION CERTIFICATE

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash	-	Sha256

algorithm		
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Name of the website owned by the PSP identified in the attribute by "O"]
	G =	[First name of the PSP representative or authorized person]
	SN =	[Surname name of the PSP representative or authorized person]
	SERIALNUMBER =	[Identifier of the PSP representative or authorized person. • For a Bulgarian citizen - one of the following: o PNOBG-XXXXXXXXXX for Personal ID o PASSBG-XXXXXXXX for passport number o IDCBG-XXXXXXXXX for ID card number o TINBG-XXXXXXXXX for tax number of a natural person o PI:BG-XXXXXXXXXX for ID number of a foreign citizen o BT:BG-XXXXXXXXXX for natural person number issued by B-Trust CA • For a foreign citizen – one of the following: o PNOYY- XXXXXXXXX for national identity number o PASSYY- XXXXXXXX for passport number o IDCYY- XXXXXXXXX for national ID card number where YY is the country code of the PSP representative or an authorized person under ISO 3166]
	O =	[Name of the PSP (Organization or company)]
	2.5.4.97= (organizationIdentifier)	[Authorization number of the PSP, issued by the BNB (competent national authority) with the following structure: PSDBG-BNB-xxxxxxxxxx, where xxxxxxxxxx – number from the Public Register of Payment Services Providers maintained by the BNB]]
	OU	[OV SSL]
	businessCategory	[One of the following categories: PrivateOrganization, GovernmentEntity, BusinessEntity, NoncommersialEntity]

	JurisdictionCountryName	[Jurisdiction - Country]
	JurisdictionOfIncorporationLocalityName	[Jurisdiction - Location]
	E =	[User email]
	L =	[User city]
	C =	BG or YY where YY is the code of the country under ISO 3166 where the User is registered
Public key	-	RSA(2048 bits)
SubjectAlternativeName		[DNS name]
Subject Key Identifier	-	[hash of „Public key "]
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.8 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [[2] Certificate Policy: Policy Identifier= 0.4.0.19495.3.1 (QCP-w-PSD2) [3] Certificate Policy: Policy Identifier=2.23.140.1.2.2 [4] Certificate Policy: Policy Identifier=0.4.0.2042.1.7
Enhanced Key Usage	-	Server Authentication, Client Authentication, Secure Email
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer
Key Usage (critical)	-	Digital Signature, Key Encipherment
Qualified Statements	qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semantics-identifiers (oid=0.4.0.194121.1) / id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)

	qcs-QcCompliance (qcStatement-1) qcs-QcType (qcStatement-6)	id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-web (oid=0.4.0.1862.1.6.3)	
	psd2-qcStatement (oid=0.4.0.19495.2)	PSD2QcType	rolesofPSP (0.4.0.19495.1)	One or more of the specified roles PSP_AS (0.4.0.19495.1.1) PSP_PI (0.4.0.19495.1.2) PSP_AI (0.4.0.19495.1.3) PSP_IC (0.4.0.19495.1.4)
			NCAName	BNB (Bulgarian National Bank) (Name of national competent authority – BNB)
			NCAId	PSDBG-BNB-xxxxxxxxxx (ID of national competent authority – BNB)
	qcs-QcPDS (qcStatement-5)	id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/psd2_pds_en.pdf language=en	

5 PUBLICATION AND REGISTRATION RESPONSIBILITIES

5.1 PUBLIC REGISTER

See section 2.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

5.2 PUBLIC REPOSITORY

See section 2.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

5.3 PUBLICATION OF CERTIFICATE INFORMATION

See section 2.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

5.4 FREQUENCY OF PUBLICATION

See section 2.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

5.5 ACCESS TO THE REGISTER AND REPOSITORY

See section 3.6 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

6 IDENTIFICATION AND AUTHENTICATION

6.1 NAMING

See section 3.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

6.2 INITIAL IDENTIFICATION AND AUTHENTICATION

See section 3.2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

In addition to the applicable requirements (section 3.2) of the above document, BORICA as a QTSP:

- Shall perform verification of the specific data of PSD2 provided by the applicant for the certificate (authorization number, role(s), name of the national competent authority) using authentic information from the national competent authority (the BNB) (e.g. in a Public Register of Payment Service Providers);
- should apply the specified requirements, if any, published by the national competent authority (the BNB);
- Shall issue qualified certificates for PSD2 only to legal persons.

6.3 IDENTIFICATION AND AUTHENTICATION FOR CERTIFICATE RENEWAL

According to this Policy BORICA as a QTSP does not renew PSD2 Qualified Certificates of a PSP.

6.4 IDENTIFICATION AND AUTHENTICATION FOR SUSPENSION

See section 3.4 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

In addition to the applicable requirements (section 3.4) of the above document, BORICA as a QTSP:

- Shall immediately notify the National Competent Authority (BNB) of the PSP's request for suspension of the certificate including the reason
- Shall immediately notify the BNB of the resumption of a suspended certificate
- Shall use a bilaterally coordinated email address provided by the BNB for communication exchange of notifications.

6.5 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION

See section 3.5 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).
In addition to the applicable requirements (section 3.5) of the above document, BORICA as a QTSP:

- Shall accept a request to terminate a certificate only from the national competent authority (BNB) as the owner of the PSD2 specific data; the request shall include the reason for revocation;
- Shall use a coordinated and secure communication channel for exchange between the two parties for accepting a revocation request;
- shall verify the authenticity and integrity of the revocation request and the reason for revocation;
- may decide not to take actions on revocation if the reason is not provided or the reason is not within the responsibility of the national competent authority (BNB);
- shall revoke the certificate if any of the following conditions are met:
  - the PSP authorization has been withdrawn
  - the authorization number of the PSP has been changed
  - the name or the identifier of the competent authority has been changed
  - a role of the PSP included in the certificate has been canceled
  - revocation is required by law;
  - other condition specified in the Policy or Practice Statement of the QTSP.
- Shall provide an e-mail address for accepting notifications by the competent authority (BNB) regarding changes to Regulatory Information for the Payment Services Provider that may affect the validity of its certificates; the content and format of these notifications is coordinated between the two parties as the QTSP should verify the source of their authenticity.

6.6 IDENTIFICATION AND AUTHENTICATION AFTER REVOCATION

See section 3.6 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS) and section 6.2 of the present document.

6.7 PUBLICATION AND REGISTRATION RESPONSIBILITIES

See section 2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

In addition to the applicable requirements (section 2) of the above specified document, the QTSP BORICA:

• Uses a bilaterally coordinated and provided by the BNB for secure communication exchange of notifications

• If BORICA AD has been provided with such an e-mail address to inform the national competent authority (the BNB), identified in a newly issued certificate, the QTSP shall send to that e-mail address information about the contents of the certificate in plain text, including the serial number of the certificate in hexadecimal format, the contents of the field for the Subject DN and the Issuer DN, the period of validity of the certificate, as well as contact information and instructions for requesting revocation and a copy of the file of certificates (.cer). It shall immediately inform the national competent authority (the BNB) of the PSP's request for revocation of the certificate and the reason thereof.

7 OPERATIONAL REQUIREMENTS AND PROCEDURES

BORICA through the RA/LRA, within a Service Agreement, provides the following operational procedures for qualified trust cervices applicable to the qualified certificates under this Policy:

- registration of issuance application;
- processing issuance application;
- QC issuance;
- QC delivery;
- use of the key pair and the QC;
- QC suspension/reactivation;
- QC revocation
- QC status.

These operating procedures are common to QSealC PSD2 and QWAC PSD2. BORICA, through RA/LRA, allows a Payment Service Provider to terminate the contract for certification services between them.

7.1 CERTIFICATE APPLICATION

See section 4.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS) and section 6.2 of the present document.

7.2 ISSUANCE PROCEDURE

See section 4.2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS) and section 6.2 of the present document.

7.3 CERTIFICATE ISSUANCE

See section 4.3 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

7.4 CERTIFICATE ACCEPTANCE AND PUBLICATION

See section 4.4 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS), and section 6.7 of the present document.

7.5 KEY PAIR AND CERTIFICATE USAGE

See section 4.5 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

7.6 CERTIFICATE RENEWAL

Under this Policy, the Provider shall not renew Qualified Certificates for Advanced Electronic Signature/Seal.

7.7 REPLACEMENT OF CRYPTOGRAPHIC KEY PAIR

See section 4.7 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

7.8 CERTIFICATE MODIFICATION

See section 4.8 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

7.9 CERTIFICATE REVOCATION AND SUSPENSION

See section 4.9 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS) and section 6.4 and 6.5 of the present document.

7.10 CERTIFICATE STATUS

See section 4.10 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

7.11 TERMINATION OF CERTIFICATION SERVICE AGREEMENT

See section 4.11 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

7.12 KEY RECOVERY

See section 4.12 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

8.1 PHYSICAL CONTROLS

See section 5.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.2 PROCEDURAL CONTROLS

See section 5.2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.3 STAFF QUALIFICATION AND TRAINING

See section 5.3 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.4 LOGGING PROCEDURES

See section 5.4 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.5 ARCHIVING AND ARCHIVE MAINTENANCE

See section 5.5 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.6 KEY CHANGEOVER

See section 5.6 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.7 KEY COMPROMISE AND DISASTER RECOVERY

See section 5.7 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.8 COMPROMISE OF A PRIVATE KEY

See section 5.8 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

8.9 PROVIDER TERMINATION

See section 5.9 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9 TECHNICAL SECURITY CONTROL AND MANAGEMENT

9.1 KEY PAIR GENERATION AND INSTALLATION

See section 6.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.2 GENERATION PROCEDURE

See section 6.2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.3 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CONTROLS

See section 6.3 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.4 OTHER ASPECTS OF KEY PAIR MANAGEMENT

See section 6.4 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.5 ACTIVATION DATA

See section 6.5 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.6 SECURITY OF COMPUTER SYSTEMS

See section 6.6 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.7 DEVELOPMENT AND OPERATION (LIFE CYCLE)

See section 6.7 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.8 ADDITIONAL TESTS

See section 6.8 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.9 NETWORK SECURITY

See section 6.9 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.10 CERTIFICATION OF TIME

See section 6.10 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

10 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

10.1 PERIODIC AND CIRCUMSTANTIAL INSPECTION

See section 8.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

10.2 QUALIFICATIONS OF THE INSPECTORS КВАЛИФИКАЦИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА

See section 8.2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

10.3 RELATIONSHIP OF THE INSPECTING PERSONS WITH THE QTSP

See section 8.3 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

10.4 SCOPE OF THE INSPECTION

See section 8.4 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

10.5 DISCUSSION OF RESULTS AND FOLLOW-UP ACTIONS

See section 8.5 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11 BUSINESS AND LEGAL ISSUES

11.1 PRICES AND FEES

See section 9.1 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.2 FINANCIAL LIABILITY

See section 9.2 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.3 CONFIDENTIALITY OF BUSINESS INFORMATION

See section 9.3 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.4 PERSONAL DATA PROTECTION

See section 9.4 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.5 INTELLECTUAL PROPERTY RIGHTS

See section 9.5 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.6 RESPONSIBILITY AND WARRANTIES

See section 9.6 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.7 DISCLAIMER

See section 9.7 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.8 LIMITATION OF LIABILITY OF THE PROVIDER

See section 9.8 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.9 INDEMNITIES FOR THE PROVIDER

See section 9.9 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.10 TERM AND TERMINATION

See section 9.10 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.11 NOTICES AND COMMUNICATION BETWEEN PARTICIPANTS

See section 9.11 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.12 AMENDMENTS TO THE DOCUMENT

See section 9.12 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.13 DISPUTE SETTLEMENT (JURISDICTION)

See section 9.13 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.14 GOVERNING LAW

See section 9.14 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

11.15 COMPLIANCE WITH APPLICABLE LAW

See section 9.15 of the current version of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).