Public Document

DISCLOSURE STATEMENT

for B-TRUST® QUALIFIED CERTIFICATES IN COMPLIANCE WITH PSD2

(B-Trust QCP-PSD2 QSealC and QWAC)

Version 1.0

January 13, 2019

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	13.01.2019	Approved	Initial release.

CONTENTS

This document is the PKI Disclosure Statement of the Qualified Trust Service Provider (QTSP) BORICA AD concerning the Qualified Electronic Seal and Website Authentication Certificates of Payment Service Providers in Compliance with PSD2 (Qualified certificates under PSD2).
This document does not substitute or replace the Policy and Practice Statement of the QTSP, according to which these qualified certificates are issued and maintained, it is rather informative and is based on the structure defined in Annex A of the document ETSI TS 319-411-1.

1. Contact Information

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

2. Types of Certificates, Identification Procedure and Usage

2.1. Types of Certificates

This Statement applies only to the Qualified Trust Services provided by BORICA for the Qualified Certificates of Payment Service Providers in compliance with PSD2. (Certificates under PSD2).

BORICA as a QTSP issues and maintains the following types of qualified certificates of 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.

The general characteristics, profile and attributes with specific data required by PSD2 and EBA/RTS for these Qualified Certificates are in accordance with the policy of BORICA contained in the document “POLICY FOR PROVIDING QUALIFIED ELECTRONIC SEAL AND WEBSITE AUTHENTICATION CERTIFICATES TO PAYMENT SERVICE PROVIDERS IN COMPLIANCE WITH PSD2”.

2.2. Identification Procedure

A qualified certificate of a Payment Service Provider under PSD2 is issued only to a subject – legal person, after verification of the applicable requirements according to 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) and verification of the provided specific data of this Provider according to PSD2 (authorization number, role(s), name of the national competent authority). The verification of validity of these data uses authentic/primary information from the Public Register of the respective National Competent Authority (e.g. the BNB). The verification is carried out by the Registration Authority/Local Registration Authorities of B-Trust or by other person authorized to confirm the identity of a Payment Service Provider (Certificate Holder). In the case of a physical person related or representing a Payment Service Provider, an authorization of the person by this Provider or a record of powers form an official state or trade register is required.

The Registration Authority/Local Registration Authorities of BORICA shall identify and authenticate the information provided by the Applicant in the Application according to section 3.2 of the above document.

2.3. Usage

Qualified certificates issued by BORICA to a Payment Service Provider should only be used in compliance with the document ETSI TS 119 495, according to PSD2 and EBA/RTS**,** i.e.:

- A Qualified Electronic Seal Certificate is used to prove the integrity/completeness and correctness of origin of data (art. 35 para. 2. of the Regulation), to ensure the integrity and correctness of the account data of the Payment Service User (PSU) between the parties and to initiate the payment;
- A Qualified Website Authentication Certificate authenticates a domain, which domain name has to be a part of the certificate (article 45 and annex IV (e) of the Regulation) - in mutual (bilateral) identification and authentication during the process of establishing a secure communication channel (TLS) between the parties - ASPSP (Bank) and PSP (AISP, PISP or PIISP).

BORICA issues qualified certificates to PSP (ASPSP, AISP, PISP and PIISP). In addition it provides services for renewal, suspension/resumption and revocation of these certificates and for consistent verification of their validity via:

- CRL or via Online Certificate Status Protocol (OCSP), and
- compliance of the specific attributes (authorization/license, role(s), and name of national competent authority) in the current Public Register of the Competent Authority.

3. Limited liability

The financial guarantee for BORICA in respect of individual event is BGN 600,000 and the total amount of the financial guarantee for all these events cannot exceed the amount of BGN 600,000. The financial liability refers to 12-month periods, which is equivalent to the calendar year.

In order to manage the performance of B-Trust and for effective control over users and staff, all events occurring in B-Trust systems for issuing and managing Qualified Certificates of Payment Service Providers that have a significant impact on security are recorded in journals.

In particular, event logs of B-Trust include: registration, issuance, revocation, and temporary suspension of certificates, renewal procedures, validation of certificate status, key generation, and other events that have a significant impact on security, and the normal operation of B-Trust.

4. Obligations of Payment Service Providers (Certificate Holders)

The Payment Service Providers should act in accordance with the common Policy (B-Trust CP-eIDAS) and Practice Statement (B-Trust CPS-eIDAS), the specific Policy for qualified certificates in compliance with PSD2, and the respective Service Agreement, which they conclude with BORICA. In this context the Holders are responsible to:

- have basic notion and understanding of proper use of cryptography with public keys and certificates;
- inform themselves about and accept the terms and conditions of the B-Trust Policy for qualified certificates in compliance with PSD2 and other relevant requirements and agreements;
- provide only accurate identification information without errors, omissions or misuse;
- provide a properly filled in and personally signed registration form (Application);
- provide the necessary documents with information on the specific attributes (authorization number, role/s, competent authority) in these certificates as well as a document of representation and identity;
- verify the contents of the issued certificate prior to initial use and avoid using it if it contains misleading or untrue information;
- ensure full control over the private key by not sharing personal codes and/or passwords;
- notify the Registration Authority/Local Registration Authorities of BORICA for any change in the information included in the certificate or any change of circumstances that will make the information in the certificate misleading or untrue;
- terminate the use of the certificate immediately if any information included therein is misleading or untrue or if there is a change in circumstances that makes the information in the certificate misleading or untrue;
- notify the Registration Authority/Local Registration Authorities immediately of any suspected or actual compromise of the private key, requesting the certificate to be terminated/revoked;
- stop using certificates immediately:
    - on expiry or revocation of a certificate, or
    - in any suspicion or actual disclosure of the private key corresponding to the public key in this certificate as well as immediately remove this certificate from the devices and/or the software on which it was installed;
- not to use the private key corresponding to the public key certificate to sign other certificates да използват частния ключ, съответстващ на удостоверението за публичния ключ, за да подписват други удостоверения;
- protect the private key from unauthorized access.

The private keys of the qualified PSD2 certificates are generated by the Payment Service Providers or at an office of BORICA in the presence of an authorized person who will only have control/access to them.

5. Relying Party Obligations for Verifying Certificate Status

Relying parties as PSP (ASPSP, AISP, PISP and PIISP) should use their qualified certificates under PSD2 only in accordance with the terms and conditions set out in the Policy of BORICA for those certificates (document “POLICY FOR PROVIDING QUALIFIED ELECTRONIC SEAL AND WEBSITE AUTHENTICATION CERTIFICATES TO PAYMENT SERVICE PROVIDERS IN COMPLIANCE WITH PSD2”). It is their responsibility to verify the legal validity and the applicable law of these certificates. Before trusting information from a Payment Service Provider's certificate, the ASPSP (the Bank) as a relying party should check the validity of the certificate, whether it has been revoked/suspended using the response/result of B-Trust CRL or OCSP, and the compliance

of the specific attributes under PSD2 and RTS / EBA with those in the Register of the Competent Authority (BNB).

Each party to the payment transaction (as a relying party) shall undertake to:

- verify that the electronic seal has been created using the private key corresponding to the public key in the Holder's certificate issued;
- verify that a sealed message/document has not been changed after sealing;
- verify accurately and correctly (using application software/devices) the compliance with the level trust of the accepted certificates with the security level of cryptographic operations for the electronic print and the website authentication;
- consider an electronic seal or certificate invalid if it is not possible to determine the validity of the seal or the website authentication certificate with the help of application software and/or devices or if the result of the verification is negative;
- trust only those Qualified Certificates that are used in accordance with the policy declared, are relevant to the scope of applicability specified by the Relying Party and their valid status has been verified based on an updated CRL or the OCSP service of B-Trust and on the basis of an up-to-date Register of the National Competent Authority (BNB) under PSD2.

6. Limited Warranty and Disclaimer/Limitation of Liability

BORICA declares and guarantees the following:

- the services for issuing and maintenance of qualified certificates of Payment Service Providers and the Document Repository are in conformity with the Common Practice Statement and Policy (B-Trust CPS/CP-eIDAS) regarding these certificates;
- at the time of issuance of these certificates, a procedure is applied to verify the accuracy of the information contained in the certificate before it is issued and initially used;
- a procedure is applied to reduce the probability that the information contained in the certificate is misleading/incorrect;
- 24/7 maintenance of publicly accessible and up-to-date document information;
- performance of identification and authentication procedures in accordance with the Common Practice and Policy for these certificates as well as internal procedures and operations for certificate issuance and maintenance;
- providing certificate management services, including posting, suspension, resumption, and revocation in accordance with the Practice and Policy for these certificates.

BORICA shall not take responsibility for:

- SERVICE unavailability due to natural disasters, war, telecommunications/energy disturbance, etc.;
- Improper/unauthorized use of the certificates or their use outside the scope of the Policy.

Limitations of liability include:

- BORICA is not responsible for Holders (Payment Service Providers) or any authorized person by them in cases where such liability is the result of their negligence, fraud or willful misconduct;

- BORICA is not responsible for the use of PDS2 certificates or related pairs of public key/private key for other purposes outside the scope under the Policy specified in the certificates unless the use is in accordance with this Policy;
- The Holders (Payment Service Providers) shall compensate the QTSP from and against any such liability and resulting costs and claims;
- BORICA is not responsible for any direct or indirect damages to any party caused as a result of an uncontrolled breach of the trust services provided to Payment Service Providers;
- Payment Service Providers are responsible for any form of invalid information contained in the certificates to the respective Relying Party, although this information has been accepted by B-Trust;
- The Holders (Payment Service Providers) shall compensate the respective Relying Party that has suffered losses as a result of breach of the Service Agreement on their part.

7. Applicable Agreements, Policy and Practice Statement

The document B-Trust CPS-eIDAS can be found in the B-Trust repository of documents at https://www.b-trust.bg/documents.

A Service Agreement concerning Payment Service Providers and an optional Agreement for qualified validation of certificates under PSD2 can also be found on the above B-Trust web address.

8. Privacy Policy/Statement

BORICA fully complies with the Personal Data Protection Act and other applicable legislation of the Republic of Bulgaria.

Any information about Holders (Payment Service Providers) which is not disclosed through the qualified certificates issued by B-Trust or through the CRLs is considered personal information. All the information contained in a qualified certificate issued by B-Trust, in CRLs of B-Trust, or provided by a publicly available service, shall not be considered confidential.

B-Trust keep all events relating to the lifecycle of keys managed by B-Trust for a period of ten months, then any certificate based on these records ceases to be stored.

9. Refund Policy

BORICA strives to provide the highest level of quality of the certification services it offers and provides to Payment Service Providers. Any Provider (Holder) may request revocation/termination of a certificate and refund of their fee, if they are not satisfied with the B-Trust services, but only if B-Trust fails to fulfill its obligations defined in the Service Agreement and in this document.

10. Applicable Law, Complaints and Dispute Resolution

The operational activity of B-Trust follows the general rules set out in the Policy and Practice Statement (B-Trust CPS/CP-eIDAS), and is in line with the applicable regulatory framework of the Republic of Bulgaria and applicable international acts. Disputes related to qualified certificates of Payment Service Providers shall be settled initially through a conciliation procedure. If the complaint is not settled within 30 days of the commencement of the conciliatory process, the parties may refer the dispute to the appropriate court. In the event of disputes and complaints arising after the use of an issued certificate or a service provided by B-Trust, The Payment Service Providers shall undertake to notify BORICA of the cause of the dispute or complaint.

11. Conformity assessments, trust marks/logos, and audit

Audits to verify conformity with procedural and legal provisions and conformity with the Practice Statement of the QTSP and the document “POLICY FOR PROVIDING QUALIFIED ELECTRONIC SEAL AND WEBSITE AUTHENTICATION CERTIFICATES TO PAYMENT SERVICE PROVIDERS IN COMPLIANCE WITH PSD2”, are performed every 24 months by an Authority for Conformity Assessment, based on Art. 20 of REGULATION 910/2014 EU (eIDAS).

The results of each regular audit are published on the B-Trust webpage, through the respective "trust mark".

12. Document Identification

This document is registered by B-Trust and is identified by an object identifier (OID): 1.3.6.1.4.1.15862.1.6.8

13. Local Registration Authorities

B-Trust offices of BORICA (Local Registration Authorities) accept applications/requests for issuance of qualified certificates for electronic seal and website authentication form Payment Service Providers after verification of their identity. The list of B-Trust offices of BORICA is published on the B-Trust website at: https://www.b-trust.bg/contacts .