BORICA
BANK SERVICES

B-TRUST QUALIFIED CLOUD QES/REMOTE QSCD SERVICE OF BORICA AD (CQES/RQSCD)

SERVICE MANUAL

Version 2.0

March 1, 2020

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	18.04.2017	Approved	Initial release
2.0	Dimitar Nikolov	01.03.2020	Approved	Text corrections

CONTENTS

1 SCOPE AND USE

This document:

- Has been developed by "BORICA" AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- contains the security requirements of the Cloud QES service (the SERVICE) in accordance with EU Regulation 910/2014 and the applicable technical specifications: EN 419 241-1/2/3, EN 419 221-5, and ETSI TS 119 431 for this SERVICE, operated by the Qualified Trust Service Provider (QTSP) BORICA AD (the Provider);
- follows the general policy and practice statement of the Provider in providing QES and their Qualified Certificates, including certain specific requirements regarding the Cloud QES;
- should be used together with the B-Trust CPS-eIDAS (the Provider's Practice Statement) and B-Trust CP-eIDAS (the Provider's Policy) documents when auditing the SERVICE to establish compliance of the Provider's activity with the regulatory framework;
- serves to assess the activity of the QTSP BORICA AD to provide Cloud QES in compliance with Regulation 910/2014;
- uses or refers technical specifications regarding the SERVICE;
- may be changed by the QTSP and any new version of this document repeals the previous one.

The following are outside the scope of the document:

- The technical aspects of formats, syntax, e-signature encoding, specific formats, profiles and encoding of the container of documents signed with cloud QES;
- The processes of signing i.e. generating the container of the cloud QES;
- The legal applicability (applicability rules) of long term preservation of cloud QES for specific business purposes.

2 INTRODUCTION

Until the approval and entry into force of the Regulation EU 910/2014 (eIDAS), the Holder of the signature (Signatory) had to submit a smart card with a QES to each signing service requiring a legally valid signature. The smart card provides, on the one hand, strict proof of identity and sole control for the Signatory and, on the other hand, signature creation functionality on the card. This requirement makes the use and management of smart cards very difficult and financially inefficient both for Users (Signatories and Relying Parties) and for Providers of QES, especially when the scope of e-signature affects many Users. The result is a low level of use of smart cards for electronic signing with QES in Bulgaria (and in the EU).

Regulation 910/2014 (eIDAS) introduces an important alternative to smart cards by enabling Trust Service Providers (TSP) to hold the signature keys on behalf of their users. By rationalizing the legal and technical framework for the electronic signature for the purpose of synchronizing and cross-border interoperability of the electronic signature, the Regulation maintains the strict technical requirements for cryptographic features and functions of QES, but in particular establishes the following:

(51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

The acceptance and validation of such functionality is known as Remote Signing (Server Signing, Cloud Signing). Instead of signing with smart cards, users can operate with a remote service to sign with a cloud QES at the QTSP, which includes a certified HSM. With the remote signing, users safely enter their credentials and sign documents using phone, browser, or other device.

The certified HSM (QHSM) with appropriate software environment at the QTSP such as Remote QSCD (RQSCD) maintains the Cloud QES service by performing the following functions:

- Securely encrypts/protects the authorization data (credentials) of the user;
- Creates and stores signing key (the private key) of each user;
- Ensures that a document will be signed only with the authorized user's signing key, i.e. this key is under the sole control of the signer;
- Generates the digital signature (PKSC#1).

In the near future, the prevailing approach for remote signing will be through remote QSCD (HSM) at the QTSP, and mobile devices (smartphones, tablets, etc.) of the Users.

3 LEGAL ASPECTS

The eIDAS Regulation introduces legal rules that define the following factors to guarantee the reliability/credibility of remote signing services:

- A certified HSM as a remote QSCD that holds the signing (private) key of the User;
- Signature activation - the process of authentication and subsequent activation of the private key; it is important to ensure that this process is under the sole control of the User at any time. The security of the activation of the private key depends on functionality provided by an external application or by an internal code in the HSM, these two options respectively referring to security level 1 and level 2 of the sole control (according to the technical specifications for remote signing, in compliance with the Regulation);
- Security of the user's personal smart device; personal devices such as smartphones shall be protected against malware and shall have controlled access, for example, by using a PIN code. If the smartphone stores the authentication key or biometric information, a trust factor may be required.
- A QTSP, which operates/manages remote signing service as a part of wider range of Qualified Trust Services by this Provider. The regular audits ensure the trust in and credibility of the QTSP. These audits assess the security of the entire Infrastructure of the Provider, including Physical and Operational Measures and the ability of the TSP to meet the expected functional requirements of the Remote Signing Service.

Three of the above factors are covered by the two requirements contained in the Regulation:

- Annex II (Requirements for Qualified Electronic Signature Creation Devices) and the additions provided by the technical specifications EN 419 241-1/2/3 and EN 419 221-5, and those of ETSI TS 119 431-1/2 and TS 119 432;

- The requirement for the QTSP to be audited regularly (Article 20, Supervision of qualified trust service providers).

4 STANDARDS/TECHNICAL SPECIFICATIONS FOR REMOTE SIGNING

In support of the remote signing service with QES, in accordance with the Regulation 910/2014 (eIDAS), the following decisions and technical standards have been published:

- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council;
- ETSI TS 119 431-1/2 - TSP service components operating a remote QSCD;
- ETSI TS 119 432 - Protocols for remote digital signature creation;
- ETSI TS 419 241 (Server Signing);
- ETSI EN 419 241-1, based on TS 419 241;
- ETSI EN 419 241-2 PP TSCM;
- ETSI EN 419 241-3 PP SAD+SAM (PP Signature Activation Module for Remote QSCD).

ETSI TS 119 431-1 defines the required components of the platform for generating a remote (digital) signature (RQSCD) at the QTSP, while ETSI TS 119 431-2 defines the components for creating the container of the Cloud QES, i.e. of the document signed with Cloud QES. The two parts of this document together allow the QTSP to specify, build and operate a complete service for remote signing of e-documents (data objects) with Cloud QES.

ETSI TS 432 defines the protocols of interaction (exchange) of an application platform with a platform for remote signing of e-documents (data objects) with Cloud QES.

ETSI EN 419 241-1 identifies two levels of “sole control assurance”.

Level 1 is based on a Server Signing Application Service (SSAS), which ensures that the relevant (private) key for the signature is selected. The functionality that supports signature activation and provides personalized control through the so-called "delegated" authentication is executed as part of the SSAS service on the server. Any HSM certified as a QSCD in accordance with the Regulation may be used (for example, according to EN 419 221-5).

In order to ensure Level 2 of secure sole control, the signature activation shall be performed with a code (SAM/Signature Activation Module or SCC/Sole Control Code) in HSM. This code is certified for the same level of security as the common cryptographic functions of the HSM. Signature activation data is transmitted in secure form from the personal smart-device of the signer to the SAM/SCC in HSM to ensure the sole control on the signature key without being impaired even if SSAS component on the server of the QTSP is compromised.

EN 419 241-2 (PP TSCM) covers the security requirements (protection profile/ PP) on the remote QSCD, equivalent to those in Annex II of the Regulation.

EN 319 241-3 (PP SAD + SAP) specifies the security requirements (protection profile/ PP) regarding the Signature Activation Data (SAD) management and Signature Activation Protocol (SAP) operation to guarantee Level 2 of sole control assurance of the Signatory in accordance with Annex II of Regulation No. 910 / 2014.

The two parts of EN 419 241-2/3 and EN 419 221-5 together certify the system/device for remote qualified electronic signature/seal (Remote QSCD/ RQSCD) and comply with the requirements of

Regulation EU 910/2014 regarding QES: *electronic signature creation data is reliably protected by the legitimate Signatory (sole control) against use by others, while the generation and management of the signature-creation data (the private key) is performed by a qualified trust service provider on behalf of the Signatory*.

5 CONCEPT

The card (smart card) QES as a legally valid e-signature meets three mandatory conditions/requirements under Regulation EU 910/2014: (1) the private key must be securely stored and protected in a QSCD, (2) is used under the sole control of the Signatory, and (3) its corresponding certificate is qualified. The first two requirements for a secure QES, implicitly referring to the smart card as a QSCD, are in conflict with the more convenient, easier and more cost-effective application and use in practice of the legally valid signature, i.e. prevent its distribution.

The dilemma “secure QES – convenient and easy to use” reflects mostly on the Signatory, but also affects the other parties in the process of signing – e-service Providers, Relying Parties and Trust Service Providers.

The Cloud/Server QES concept eliminates this dilemma/conflict by providing centralized storage and management of private keys (for e-signatures) at the QTSP in a highly secure environment and strict administrative and operational procedures with physical and logical protection. The Signatory keeps full and sole control over his private key through a secure/protected 2FA (2-Factor Authentication) online authentication mechanism (Time-Based One-Time-Password/TOTP). When this mechanism is implemented through a mobile device (smartphone or tablet with mobile application), the Signatory gets "mobility" of the QES.

The "Mobility" as a feature of the Cloud QES does not mean that it is generated on the respective mobile device (smartphone, tablet, etc.), it only serves to activate the creation of QES on a remote server platform (RQSCD) at the QTSP. The “Mobility” addresses the Signatory who is already "exempted" from the specific technical requirements for using the QES (to have a smart card and reader and install the appropriate drivers for them) while maintaining/guaranteeing the same legal and technical requirements for the security of the legally valid e-signature.

The "Cloud QES" is a concept that "moves"/virtualizes the smart card (local QSCD) for QES (of the Signatory) in HSM on a server platform (RQSCD) at the QTSP. A “virtual slot” is allocated in the RQSCD as a remote resource of the Signatory with equivalent cryptographic parameters and characteristics of the smart card (local QSCD). The physical distance of the Signatory and his "Remote QSCD" regarding the sole control is compensated by using two separate communication channels - via the Internet and via the mobile network, used for authentication (2FA) of the Signatory and for activating the creation/generation of the signature by a PIN code. By duality of the communication channels the characteristics of SAP (Signature Activation Protocol), SAD (Signature Activation Data) and SAM (Signature Activation Module) are supported according to the technical specifications specified under section 4 of this document.

The 2FA mechanism ('something I have + something I know') in the Cloud QES concept performs the same role for the personal access to and control of the signature creation data (i.e. of the private key), as that of the PIN code for the card QES (QES on a smart card); i.e. it personally authenticates the Signatory. In this case, the technical factor 'I have a smart card' is replaced by 'I have a registered smartphone', and the personal factor ‘I know PIN’ is replaced by 'I know Password/PIN for signing', which are under the sole control of the Signatory, when creating/generating the signature in the HSM on the server (RQSCD). The 'have' factor is guaranteed by an installed and activated mobile application on the smartphone identifying the Signatory’s smartphone by a unique ID (App_ID) and the 'know' factor is guaranteed by encrypted activation data (PIN) in an encrypted session of the

Signatory to the server with HSM (RQSCD). The HSM on the server will generate QES only after successful authentication of the Signatory to the SSAS, and to the HSM respectively ("delegated" authentication) by both codes - the TOTP code for 2FA and the PIN code for the private key on the two independent 'channels' (Internet and Mobile Internet).

The Cloud QES concept by ‘moving’ the smart card (local QSCD of the Signatory to a RQSCD HSM on the server of the QTSP, requires additional organizational and technical procedures that ensure two-factor authentication and data protection for creating QES with a level of security equivalent to that of the smart card (local QSCD).

According to this concept, a 'Cloud QES' means QES of a Signatory that uses a mobile smartphone with the mobile application and mobile internet to activate remote generation of a QES on a RQSCD (a server platform with HSM) at the QTSP, through a ‘delegated’ two-factor authentication of the Signatory.

The Creation/Generation of a Cloud QES brings down the Signatory’s local environment to:

- a standard browser on a PC with Internet access;
- a smartphone with installed and initialized mobile application, successfully registered on the RQSCD (server with SSAS and HSM) at the QTSP.

The need for QES equipment (smart card, reader and drivers) is eliminated, as well as the installation and maintenance of the software of the QES equipment at the client.

6 CONCEPTUAL MODEL

Figure 1 presents the most common conceptual model of remote (server) signing with QES. The role of the RQSCD in the model is executed by the SSAS and the HSM on the server at the Provider. The organizational and technical requirements and measures that guarantee the sole control assurance are missing.

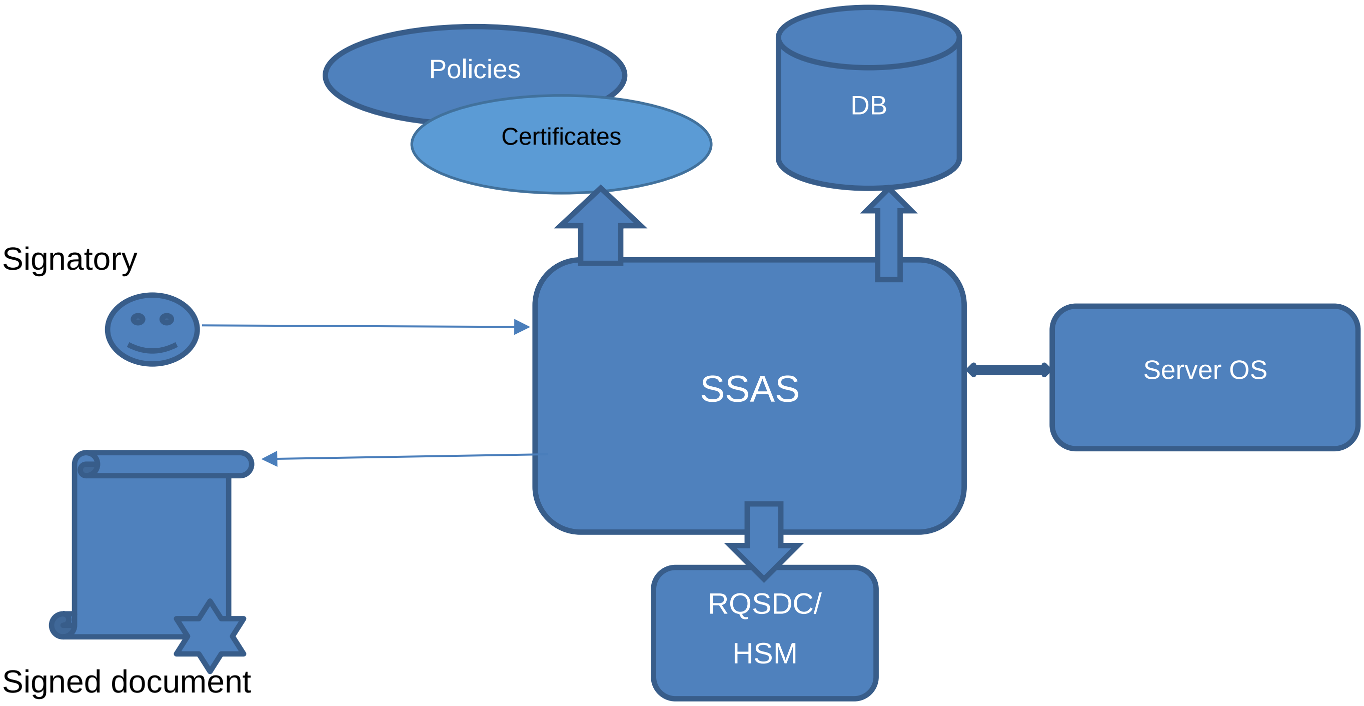

Figure 1. A common conceptual model of remote signing

Additional technical and organizational measures are introduced to this conceptual model for strong authentication of the Signatory, based on dynamic two-factor authentication, where the TOTP-code represents the first factor, and the second factor is the owned smartphone with activated registered mobile application.

The private key is protected in the SSAS, so the key does not appear explicitly outside the HSM. Access to the use of the key is possible only after the successful authentication of the Signatory (there should be procedures to guarantee that system administrators, including administrators of the HSM, cannot access the authentication data of the Signatory – password/PIN and OTP code).

Figure 2 presents a conceptual model of Cloud QES with introduced technical and organizational measures providing sole control assurance Level II.

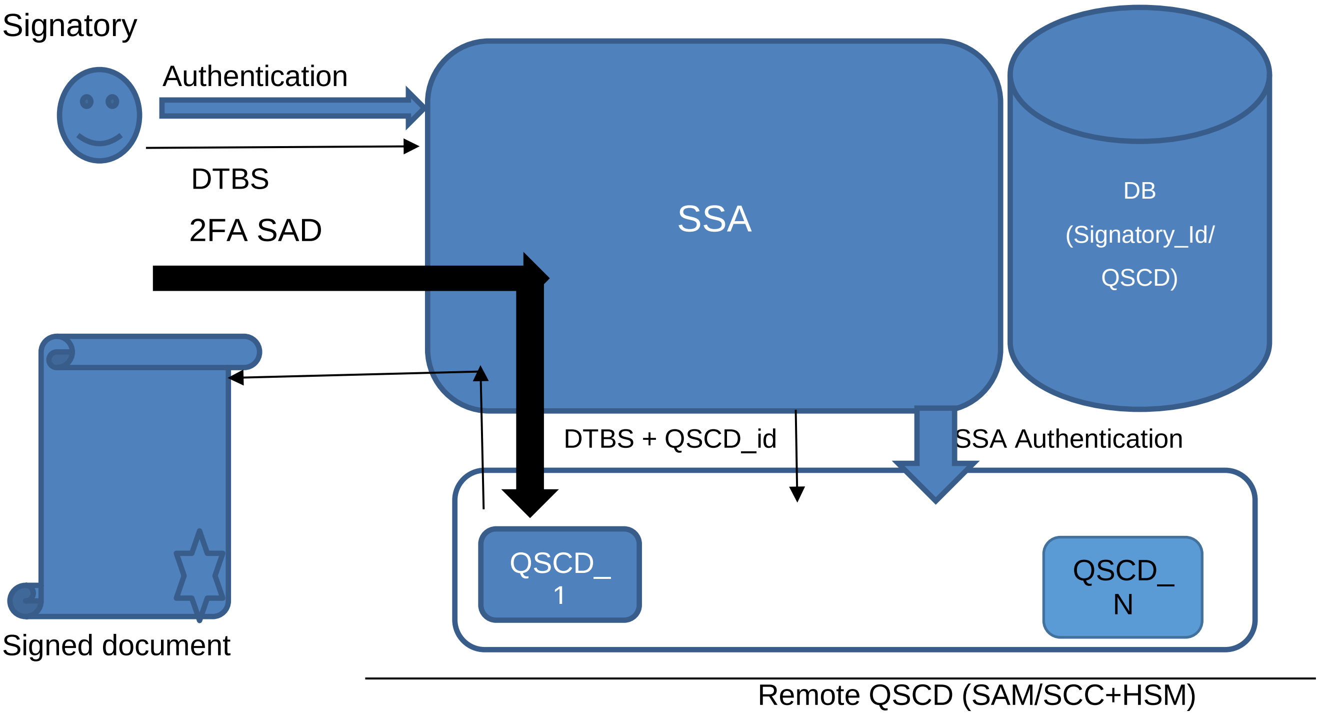

Figure 2. A conceptual model of sole control assurance Level II

Activation of a signature is done by a code (SAM / Signature Activation Module or SCC / Sole Control Code) in the HSM. This code is certified to the same level of security as the common cryptographic functions of the HSM. The technical standard EN 419 241-3 (PP SAD + SAP) specifies the secure profile of the RQSCD based on a QSCD/HSM with implemented code (SAM/SCC) in it.

Signature activation data is transmitted in a secure form directly from the personal device (PC, smartphone, tablet, etc.) of the Signatory to the SAM/SCC in the HSM via secure/protected channel for the sole control assurance of the Signatory over the signature key (private key) and inability to misuse this key even if the SSAS on the server of the QTSP is compromised.

In the practical realization of the Cloud QES concept, the QTSP BORICA AD follows the conceptual model for cloud QES with sole control assurance Level I of the data for activation of the signature (Figure 1). Sole control assurance Level I in this model is implemented through the so-called 'delegated' authentication (Holder to SSAS and via SSAS to HSM). The model is an extension of that in Figure 1 by using two separate communication channels. The one communication channel, usually via the Internet, is used for preparation of documents and sending certified request for signing to the search service application (SSA), and another communication channel the mobile network (mobile Internet) is used for activation and confirmation of the cloud QES using the personal device (smartphone).

7 FUNCTIONAL MODEL

The Cloud QES platform includes:

- Remote server component of the QTSP BORICA AD including RQSCD (SSAS and HSM) under their management and control;

- Mobile application for smartphone (for Android and iOS platforms).

RQSCD is a part of the B-Trust infrastructure identified as its object with an identifier 1.3.6.1.4.1.15862.1.6.8, which follows the common Practice Statement and Policy of the QTSP BORICA AD according to the documents: B-Trust CPS-eIDAS and B-Trust CP-eIDAS, as well as the specific conditions and requirements defined in this document. It includes two parts with the following functionalities:

- "Cloud QES Issuance" – generates the key pair for cloud QES, operates internal cryptograms for protection and security of the access to the key pair, and maintains and stores secure/encrypted private key for creating a digital signature for cloud QES;
- "Signing with Cloud QES".

The "Cloud QES Issuance" functionality uses as much as possible the current implementation of the B-Trust infrastructure, through which the QTSP BORICA AD issues and maintains the card QES (a QES on a smart card), as well as the related certification services - issuing, renewal and management (suspension/resumption, and termination/revocation) of QES certificates.

The Cloud QES maintenance/management is fully implemented through the existing functionality of the B-Trust Portal for maintenance/management of the card QES (i.e., of the Qualified Certificates for card QES) and does not use the RQSCD (SSAS and HSM).

The initial issue, renewal and management (suspension/resumption, and termination/revocation) of the Cloud QES follow the general functional requirements and the relevant procedures for QES specified in the document "CERTIFICATION PRACTICE STATEMENT FOR PROVISION OF QUALIFIED CERTIFICATES AND QUALIFIED TRUST SERVICES BY BORICA AD" B-Trust CPS-eIDAS). The present document only contains the particularities and distinctions in these functional procedures regarding the Cloud QES.

The B-Trust Mobile application is a specialized application for both mobile platforms - Android and iOS and serves to activate the creation/generation of the Cloud QES. The B-Trust Mobile application is freely available for downloading and is initialized through the Signatory's smartphone.

The RQSCD Cloud QES Platform in the B-Trust infrastructure supports two main functionalities:

- "Registration" and "Issuance" of Cloud QES – implemented through the "Cloud QES Issuance" part;
- „Signing" with Cloud QES – implemented through the "Signing with Cloud QES" part.

The "Registration" and "Issuance" functionality of the "Cloud QES Issuance" part uses the following operating components of the B-Trust infrastructure:

- Certifying Authority - issuing qualified certificates in accordance with the EU Regulation 910/2014;
- B-Trust Portal - with an additional web interface to the Subsystem for Cloud QES Issuance;
- Public Register and CRL of qualified certificates (LDAP server).

The "Signing" functionality of the "Signing with Cloud QES" uses the following operating components of the B-Trust infrastructure:

- Public Register and CRL of qualified certificates (LDAP server) and/or
- OCSP-server.

7.1 Cloud QES "Registration" and "Issuance" functionalities

The information in this part of the document should be used together with the information in B-Trust CPS-eIDAS document, in section 3 (3.2) and section 4 (4.1, 4.2, 4.3, 4.4 and 4.5).

The applicant for the Cloud QES Certification Service should register a request (e-form) for issuance of a Qualified Certificate for Cloud QES to the QTSP BORICA AD. The following option (channels) for the registration of a Cloud QES request are possible:

(1) Online initial request, from smartphone;

(2) On-line initial request, from a browser on a PC via the B-Trust website of the QTSP and a subsequent visit to an office of the QTSP;

(3) Offline initial request, on site at an office of the QTSP through an agent - employee of the Provider;

(4) On-line request, from a browser on a PC via the B-Trust Portal of the QTSP and an issued valid certificate for (card) QES.

The comparatively large amount of data to be filled in the e-form of the initial request for issuance of Cloud QES makes option (1) uneasy and inconvenient and is (currently) not supported by BORICA AD.

Options (2) and (3) are similar, except that in case of option (3) the e-form of the request for the initial issuance of Cloud QES is filled in by the Agent at the Provider's office (LRA/Local Registration Authority) in the presence of the Applicant/Signatory.

Requirements to the Applicant/Signatory:

- A smartphone (mobile platform Android or iOS) with mobile Internet;
- A personal computer with Internet access;
- Identity document(s);
- To visit a convenient office of the Provider;
- Registration number of the online request for Cloud QES (provided by the B-Trust Portal);
- B-Trust Mobile application loaded and initialized/personalized on the smartphone (*)

(*) Information on loading, personalization and registration of the B-Trust Mobile application is contained in the document “B-Trust Mobile application - User Manual”. The activation and registration of the B-Trust Mobile generate a unique ID (App_ID) and password, and register this ID in the “Cloud QES Issuance” part in the RQSCD on the cloud QES Platform.

Option (2) includes:

- The Applicant fills in the online e-form (fully or partially) and makes a request for Cloud QES issuance. He/she submits the request by sending it to the “Cloud QES Issuance” part, the request is recorded in a database (for Cloud QES) and the Applicant receives a Request Number;
- The Applicant visits an office of the Provider where the Applicant/Signatory is identified - the required documents are provided, payment is made;
- The Agent completes the request with the necessary information, the user confirms the content of the certificate for the future Cloud QES and the Agent validates the request, which is recorded in a database of Cloud QES with a "Pending" status;
- The “Cloud QES Issuance” part returns a QR code to the screen of the Agent after the entry in the database;
- The applicant scans with the smartphone the QR code containing the URI; the mobile application addresses this URI by sending an App_ID and receives an initialization data structure (2FA Shared Secret Key, a crypto key for the PIN, and account information for the Applicant); both keys are stored encrypted with the password in the mobile application;

- In the next page in the browser the Agent is invited to introduce a 2FA TOTP-code from the Applicant's smartphone to check the smartphone possession/holding; The Applicant generates a TOTP-code on his smartphone;
- The generated TOTP code from B-Trust Mobile is entered on the browser page and sent to the "Cloud QES Issuance" part where it is checked; this completes the verification on the possession of the smartphone;
- The paid Cloud QES issuance request passes to "Confirmed" status; the "Cloud QES Issuance" part sends a push notification to the mobile application with request to enter the PIN;
- The PIN for the Cloud QES is entered on the smartphone, which is encrypted with the stored crypto key for the PIN in the mobile application; the encrypted PIN is transmitted to the "Cloud QES Issuance" part of the QRSCD and participates in the process of generating the key pair for the Cloud QES and creating the public cryptograms for protection of the private key for Cloud QES through the HSM;
- The key-pair for the Cloud QES is generated and the public cryptograms for the private key of the Cloud QES are created through the HSM (which are associated with the respective APP_ID in the Cloud QES database;
- The public key for the Cloud QES participates in the follow-up procedures of the B-Trust platform for issuance of Qualified Certificate for QES (a PKCS # 10 / CSR application is formed, the issued certificate for this request is generated and signed by the B-Trust CA, the issued certificate is published in the Public Register);
- The "Cloud QES Issuance" part sends a push notification to the mobile application, or the user himself checks the status of the request in the mobile application for issued Cloud QES.

Option (4):

This option is developed and maintained in order to facilitate and accelerate the transition/ transformation from already issued and valid card QES to Cloud QES for Signatories, who wish this transition, and do not have to visit an office of the Provider. The objective is to accelerate the expansion of applicability of the Cloud QES to Users and Providers of e-services in view of the convenience and the advantages it offers to parties using the e-signature.

The functionality in this option is different from the previous version only in the first four steps:

- A Signatory of a valid card QES addresses the B-Trust WEB site in the PC browser. He/she is authenticated with his/her card QES (two-sided SSL session). The qualified certificate for this QES is retrieved from the session and the verified information is provided for the next steps;
- The browser displays the information of the Signatory of card QES and automatically a form is filled, based on which a request for Cloud QES is generated. Some data may be changed, information can be added (identifiers needed during the process of use);
- After editing (if necessary), the Cloud QES Issuance Request is recorded in Cloud QES database (account). The user receives the number of request for mobile QES;
- The same steps as in option (2) follow, except that the pages in the browser are received on the PC of the Signatory – applicant for the cloud QES, not by the Agent at the LRA.

7.2 Cloud QES "Management" functionality

The Cloud QES "Management/Maintenance" functionality includes:

- Cloud QES suspension;
- Reactivation of a suspended cloud QES;
- Cloud QES revocation.

The QTSP BORICA AD issues Qualified Certificates for Cloud QES with a validity period according to the Policy for the qualified certificates. After expiry of validity, the Cloud QES Signatory may renew the Cloud QES or apply for the issuance of a new one.

The Provider supports change of PIN and blocking/unblocking of user PIN of an issued Cloud QES.

The above specified "Management/Maintenance" functionality of the Cloud QES is performed by the B-Trust platform for QES, following the requirements and the procedures for card QES specified in the document " CERTIFICATION PRACTICE STATEMENT FOR PROVISION OF QUALIFIED CERTIFICATES AND QUALIFIED TRUST SERVICES BY BORICA AD" B-Trust CPS-eIDAS), section 3 (3.4, 3.5, 3.6), and section 4 (4.8, 4.9, 4.10).

7.3 "Signing with Cloud QES" functionality

This functionality within the scope of the "Cloud QES Usage" part of the RQSCD performs only digital signature generation (PKCS # 1) after strict authentication of the Cloud QES Signatory. The generated digital signature and the associated certificate of the public key corresponding to the private key are provided by a specified application SERVICE of the QTSP BORICA AD for signing with Cloud QES, which integrates them and forms the e-signature container according to the required/requested format of QES (CAdES, XAdES, PAdES, ASiCS/E) and class (security level) of the signature (BASELINE_B, BASELINE_T, BASELINE_LT, BASELINE_LTA). Please see the document "CERTIFICATION SERVICE FOR REMOTE SIGNING WITH CLOUD QES - POLICY AND PRACTICE STATEMENT" of the QTSP BORICA AD.

The functionality of this Service for remote signing with cloud QES may be exported as part of application systems at application e-service providers.

The formation of the e-signature container based on a Cloud QES is outside the scope of the RQSCD server component and of this document.

A document for signing (may) be stored on an application (corporate) server or on the local system (PC) of the Signatory. For the sake of confidentiality, the Service for remote signing with cloud QES is provided with a hash data for the document for signing.

The functionality of the "Signing with Cloud QES" part of the RQSCD together with the Service for remote signing with cloud QES include:

- After a User (or a Relying Party) of the Service selects an e-document for signing and provides a readable PROFILE_ID (generated based on APP_ID) from the mobile application on the smartphone of the Signatory, the hash of the document is formed, and is displayed on a page in the browser of the Signatory with a field for entering the TOTP code;
- The Signatory enters the TOTP-code generated by the mobile application;
- The browser of the Signatory is redirected to the Service for Signing, which operates with the "Signing with Cloud QES" part of the RQSCD with parameters – the identifier, TOTP, hash-data and callback URL to the Relying party;
- The "Signing" part of the RQSCD authenticates the Signatory by verifying the TOTP and sends a push notification to the mobile application with information of the document waiting for signing (hash of the document), and request to activate the generation of the (digital) signature;
- The user reviews and compares the received hash of the document with that on the browser and confirms signing by entering the PIN to activate the generation of a digital signature (PKCS#1) in the RQSCD through the HSM;
- SAP/Signature Activation Protocol provides the encrypted PIN (SAD) to the "Signing" part of the RQSCD;

- Through the entered PIN cryptographic operations are executed with the public cryptograms, created in the RQSCD when issuing the (certificate for) Cloud QES; they serve for the Signatory’s sole control over the public key for generating digital signature (PKCS#1);
- A digital signature (PKCS # 1) is generated in the HSM of the RQSCD only after successful validity verification of the qualified certificate of the public key corresponding to the addressed private key in the HSM;
- The generated digital signature (PKCS#1) together with the Qualified Certificate of the Cloud QES is provided to the Signing Service, which generates the Cloud QES container, according to the requested format and profile, respectively to the Relying Party/ User initiated the signing;
- Information of successfully signed document is displayed on the Signatory’s smartphone.

8 TECHNICAL SPECIFICATION AND REALIZATION

The practical realization of the RQSCD of the Cloud QES service is implemented according to the functional model in Section 7 of this document.

The QTSP BORICA AD plans future development of the Cloud QES Qualified Service through implementation of RQSCD with HSM + SAM/SCC Code, certified in accordance with EN 419 241-2/3.