Public document

POLICY AND PRACTICE FOR PROVIDING QUALIFIED SERVICE FOR THE MANAGEMENT OF REMOTE QUALIFIED ELECTRONIC SIGNATURE / SEAL CREATION DEVICES

Version 1

Effective: MARCH 10, 2026

CONTENTS

SCOPE AND USE

This document:

- is developed by BORICA AD, a legal entity registered in the Bulgarian Commercial Register at the Registry Agency under UIC 201230426;
- enters into force on **10 March 2026;**
- defines the requirements for the "Cloud Qualified Electronic Signature" service (remote signing) in accordance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, and the applicable technical specifications EN 419 241-1/2/3, EN 419 221-5 and ETSI TS 119 101 for this service operated by the Qualified Trust Service Provider (QTSP) BORICA AD (the Provider);
- follows the general policy and practice of the Provider for issuing Qualified Electronic Signatures (QES) and their qualified certificates, while including specific requirements related to the Cloud QES service;
- serves as a basis for the assessment of the activities of the QTSP BORICA AD in providing the Cloud QES service in compliance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183;
- uses and references applicable technical specifications related to the service;
- may be amended by the QTSP, and any new version of this document shall supersede the previous one.

STANDARDS AND TECHNICAL SPECIFICATIONS FOR REMOTE SIGNING

- 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 (eIDAS).
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates – Part 1: General requirements.
- ETSI TS 119 431 Policy and security requirements for trust service providers – Part 1: TSP service components operating a remote QSCD/SCDev (remote signing).
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation.
- ETSI TS 119 102 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures – Part 1: Creation and Validation.
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
- CEN EN 419 241 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.
- IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

For more information about this document, contact the Provider at:

41 “Tsar Boris III” Blvd.
1612 Sofia
BORICA AD
Phone: 0700 199 10
E-mail: info@borica.bg
www.b-trust.bg

1 INTRODUCTION

This document (the Policy and Practice Statement) defines the policy, practices and security requirements applied by **BORICA AD**, in its capacity as a **Qualified Trust Service Provider (QTSP)**, in the provision of **remote qualified electronic signature** and **remote qualified electronic seal** creation services.

This document describes the requirements for the management and operation of the remote signing service components, including the components operating **remote qualified electronic signature/seal creation devices (QSCD/SCDev)**, as well as the components supporting the creation of **AdES electronic signatures (SCASC)**.

This Policy and Practice Statement has been developed in accordance with **Regulation (EU) No 910/2014 (eIDAS)**, as amended by **Regulation (EU) 2024/1183**, and the relevant technical standards and specifications, including **ETSI EN 319 401**, **ETSI EN 319 411-1/2**, **ETSI TS 119 431-1**, **ETSI TS 119 431-2** and **CEN EN 419 241-1**.

The remote signing service components enable the creation of electronic signatures and electronic seals by means of secure cryptographic devices (**QSCDs**), which ensure the secure generation and storage of the private signing keys and their use under the control of the signatory.

The component supporting the creation of AdES electronic signatures (**SCASC**) provides the processing of signing requests, the preparation of the data to be signed, and the interaction with the server-side signing component (**SSASC**) and the relevant QSCD. Within this process, external trust services may be used, such as time-stamping or certificate validation services.

The remote signing service provided by **BORICA AD** enables the creation of **advanced** and **qualified electronic signatures and electronic seals**, based on **X.509 certificates** issued within the **B-Trust public key infrastructure**.

This document is intended for service users, relying parties and auditors, and its purpose is to describe the applicable policies, control mechanisms and security requirements relating to the provision of the remote creation of electronic signatures and electronic seals.

This document is structured in accordance with the framework defined in **IETF RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework**

2 DEFINITIONS AND ABBREVIATIONS

Term	Definition
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Signature Creation Application (SCA)	Application for the creation of an electronic signature.
Qualified Electronic Signature/Seal Creation Device (QSCD)	A qualified electronic signature or seal creation device that meets the requirements of Regulation (EU) No 910/2014.

Term	Definition
Relying Parties	Natural or legal persons relying on the trust services provided by BORICA AD.
Data to be Signed Representation (DTBS/R)	Formatted data used to compute the electronic signature value (e.g. a hash value).
Qualified electronic signature	An advanced electronic signature that is created by a qualified electronic signature creation device and is based on a qualified certificate.
Signature Activation Data (SAD)	Data used for signature activation.
Electronic identification (eID)	The process of using electronic identification data uniquely representing a natural or legal person.
Signature Creation Application Service Component (SCASC)	Service component of the signature creation application.
Server Signing Application (SSA)	Server-side signing application using a remote signature creation device.
Certification Practice Statement (CPS)	A document setting out the procedures and rules for the issuance, management, suspension and revocation of certificates, as well as the conditions for the provision of trust services.
Signature Creation System (SCS)	System for the creation of electronic signatures.
Signature creation data	Unique data used by the signatory to create an electronic signature.
Server Signing Application Service Component (SSASC)	Service component of the server signing application generating electronic signature values on behalf of the signatory.
Trust service	An electronic service consisting of the creation, verification and validation of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, website authentication certificates, or the preservation of such signatures, seals or certificates.
Signature Activation Module (SAM)	A signature activation module consisting of configured software executed in a protected environment.
Electronic signature certificate	An electronic attestation which links electronic signature validation data to a natural person.
Trustworthy System Supporting Server Signing (TW4S)	A trustworthy server-side signing system using signing keys under the sole control of the signatory.
AdES (digital) signature	An electronic signature in CAdES, PAdES or XAdES format.
Qualified trust service	A trust service which meets the applicable requirements of Regulation (EU) No 910/2014.
Server Signing Application Service Provider (SSASP)	Service provider offering a server signing application.
Signature Creation Application Service Provider (SCASP)	Service provider offering a signature creation application.
Remote Signature Creation Device (SCDev)	A remote electronic signature or seal creation device ensuring that the signing operation is performed under the sole control of the signatory.
Private key	A cryptographic key used to create an electronic signature or to decrypt data.

Term	Definition
Signer Interaction Component (SIC)	Component for interaction with the signatory.
Electronic identification means	A material and/or immaterial unit containing electronic identification data and used for authentication in an online service.
Qualified electronic signature certificate	A certificate issued by a qualified trust service provider which meets the requirements of Regulation (EU) No 910/2014.
Qualified trust service provider	A trust service provider providing one or more qualified trust services and having been granted qualified status by the supervisory body.
Qualified electronic seal	An advanced electronic seal that is created by a qualified electronic seal creation device and is based on a qualified certificate.
Electronic seal certificate	An electronic attestation which links electronic seal validation data to a legal person.
Public key	One part of a key pair in an asymmetric cryptosystem, used to verify an electronic signature.
Electronic seal	Data in electronic form attached to or logically associated with other data in electronic form to ensure the origin and integrity of the data.
Signature Activation Protocol (SAP)	Protocol for signature activation.
Seal creator	A legal person that creates an electronic seal.
Driving Application (DA) / Digital Identity Solution (DIS)	A controlling application organizing the processes for creation, validation and extension of electronic signatures, as well as the interaction with end users and external services.
Signatory	A natural person who creates an electronic signature.
Electronic signature value	The result of a cryptographic operation on data enabling verification of the origin and integrity of the information.
Qualified electronic signature creation device	An electronic signature creation device meeting the requirements of Regulation (EU) No 910/2014.
Qualified electronic seal creation device	An electronic seal creation device meeting the requirements of Regulation (EU) No 910/2014.
Authentication	An electronic process enabling the verification of the identity of a natural or legal person or the confirmation of the origin and integrity of data.
Identity data	A set of data enabling the identity of a natural or legal person to be established.

3 CONCEPT

A **qualified electronic signature (QES)** implemented by means of a smart card meets the main requirements of **Regulation (EU) No 910/2014 (eIDAS)**:

1. the electronic signature creation data (the private key) must be protected and stored in a **qualified electronic signature creation device (QSCD)**;
2. the use of such data must remain under the **sole control** of the signatory;
3. the signature must be based on a **qualified certificate**.

The **Cloud Qualified Electronic Signature** concept implements these requirements by means of centralized generation, storage and management of the electronic signature keys within a protected server infrastructure of the **Qualified Trust Service Provider (QTSP)**. In this model, the private keys are stored in a **hardware security module (HSM)** functioning as a **remote QSCD**.

BORICA AD provides remote electronic signature and electronic seal creation services through the implementation and maintenance of a **Trustworthy System Supporting Server Signing**, compliant with the security requirements defined in **CEN EN 419 241-1**.

The trustworthy system operates in a controlled and protected environment that includes organizational, technical and physical security measures relating to personnel management, system operating procedures, and the maintenance of the relevant technical and operational documentation. These measures are intended to ensure the reliable provision of remote electronic signature and electronic seal creation services.

The level of assurance regarding control over the use of the signing key when creating an electronic seal may differ from the level required when creating an electronic signature, depending on the applicable regulatory requirements and the relevant service policy.

The trustworthy system of **BORICA AD**, supporting server-side signing (**TW4S**), provides remote electronic signature and electronic seal creation services while ensuring that signing keys are used solely under the control of their holder.

The system supports two levels of assurance relating to control over the use of signing keys (**sole control assurance levels**) in accordance with **EN 419 241-1**:

SCAL1 – a lower assurance level of control.

At this level, signing keys may be generated, stored and used outside a hardware cryptographic module, for example in protected file structures. In such cases, the system applies additional organizational and technical safeguards against unauthorized modification, deletion or compromise of the keys.
The signing operation is authorized following successful authentication of the signatory within the **server signing application (SSA)**, which associates the signatory's authentication factors with the use of the relevant signing key.

SCAL2 – a higher assurance level of control

At this level, dedicated protected components are used to manage the signature activation process. The interaction between the **Signature Activation Module (SAM)** and the **Signer Interaction Component (SIC)**, through the **server signing application (SSA)**, results in the generation of the **Signature Activation Data (SAD)**. These data enable the signing operation to be executed on specific data to be signed. Within SCAL2, the **SAM** manages the use of the **SAD** and applies a **Signature Activation Protocol (SAP)**, which provides a level of security equivalent to that achieved by a stand-alone **QSCD**, in accordance with **Regulation (EU) No 910/2014**.

4 CONCEPTUAL MODEL

Figure 1 presents the general conceptual model of remote (server-side) qualified electronic signing. In this model, the role of the remote QSCD is performed by the HSM located at the Provider's server. The model does not yet include the organizational and technical measures required to ensure sole control assurance.

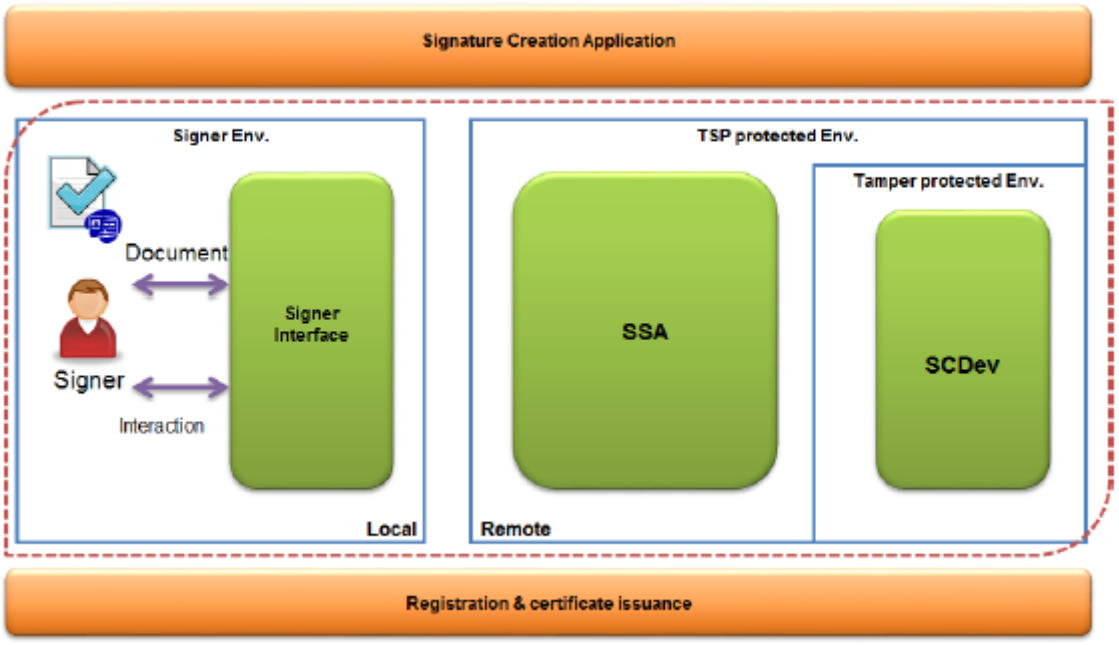


Figure 1 – General conceptual model of remote signing

Additional organizational and technical measures are introduced into this conceptual model in order to provide strong authentication of the signatory on the basis of dynamic two-factor authentication, where the **TOTP code** represents one authentication factor and the second factor is the signatory's smartphone with an activated and registered mobile application. The private key is protected within the **SSAS**, so that it never appears in plaintext outside the **HSM**. Access to the use of the key is possible only after successful authentication of the signatory. Appropriate procedures shall ensure that system administrators, including HSM administrators, cannot gain access to the signatory's authentication data, such as password/PIN and OTP code.

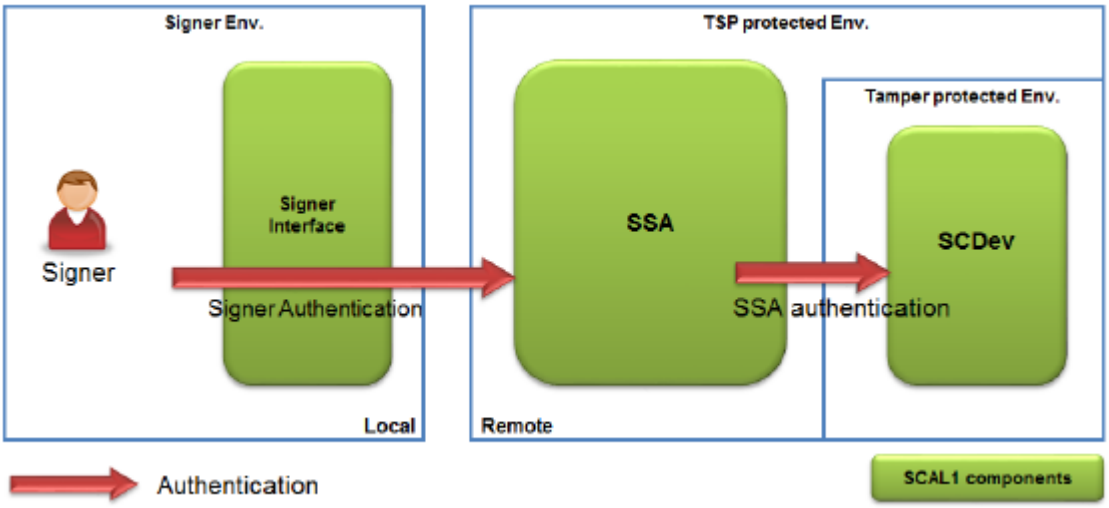


Figure 2 – Conceptual model of remote signing SCAL1

Figure 2 presents the conceptual model of the Cloud QES service with the technical and organizational measures required to provide **Level 1 sole control assurance (SCAL1)**.

At **SCAL1**, the confidentiality and integrity of the signing key are ensured by the **Signature** Creation Device (SCDev). This device stores the signing key and ensures that it cannot be extracted or used outside the protected system environment.

The activation of the signature creation device is performed by the Server Signing Application (SSA). Before the use of the signing key is authorized, the signatory must be successfully authenticated by the SSA. Once authentication is completed, the system may activate the signing key and allow signing operations to be performed on behalf of the signatory.

Within SCAL1, the activation of the key may remain valid for a defined period of time or for a defined number of signing operations. This means that, after successful authentication of the signatory, the key may be used to sign multiple documents within a predefined time period or up to a predefined number of signatures.

This model allows the server signing application to be used efficiently for batch signing, where multiple documents may be signed following a single authentication of the signatory.

This architecture may be used to create a digital signature value (for example, a hash encrypted with the private signing key) at a lower level of control assurance.

At SCAL2, the signing operation is performed through the interaction between the SIC, SSA, SAM and SCDev (HSM). The Signature Activation Data (SAD) are generated through the Signature Activation Protocol (SAP) and link together the signatory authentication, the selected signing key and the data to be signed.

The SAM, operating in a protected environment, validates the SAD and manages the activation of the signing key within the cryptographic module. In this way, the use of the signing key is ensured to remain under the sole control of the signatory in accordance with Regulation (EU) No 910/2014.

The TW4S of BORICA AD consists of a server signing application (SSA) and a remote signature creation device (SCDev) managed through the SAM. The signatory interacts with the system through the Signer Interaction Component (SIC), which establishes the link between the signatory and the specific signing operation.

Following successful authentication of the signatory by the SSA and validation of the SAD by the SAM, the signing key is activated within the SCDev and the digital signature value is generated. The generated signature is returned to the Signature Creation Application (SCA), which creates the signed electronic document.

The TW4S also supports batch signing, where one set of Signature Activation Data (SAD) may be used to sign more than one document.

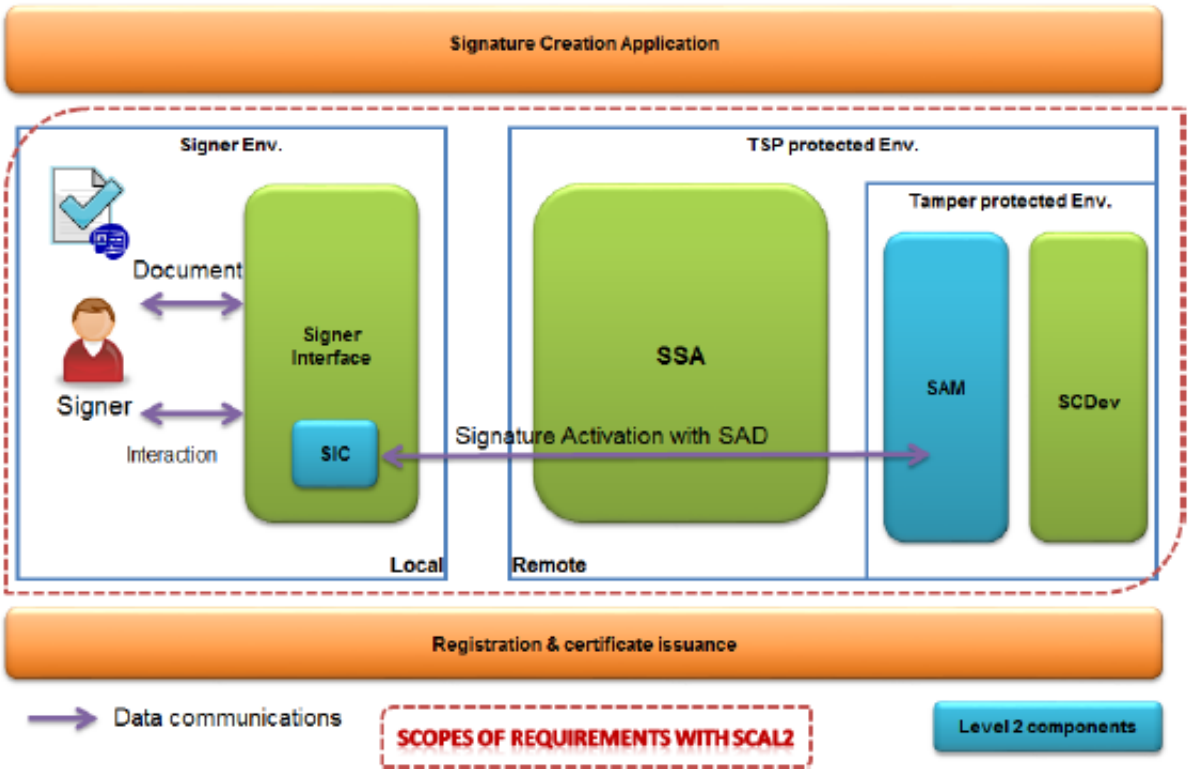


Figure 3 – Conceptual model of remote signing SCAL2

5 SERVER SIGNING APPLICATION (SSA)

The Server Signing Application (SSA) is a component of the remote electronic signature creation system through which the process of generating the digital signature value over the Data To Be Signed Representation (DTBS/R) is managed. The signing operation is performed by means of the Server Signing Application Service Component (SSASC), which uses a signing key stored in a cryptographic module (SCDev).

The signing keys are created and stored in the protected environment of the cryptographic module, and their use is authorized only after successful authentication of the signatory. The management of the activation of

the signing key is performed by means of a Signature Activation Module (SAM), which uses Signature Activation Data (SAD) for authentication of the signatory and authorization of the signing operation.

The system supports two levels of sole control over the signing key:

SCAL1 – the signing key is used following successful authentication of the signatory by the SSASC. The key activation may remain valid for a defined period of time or for a defined number of signing operations.

SCAL2 – the signing key is activated by means of the SAM, which verifies the SAD generated through the Signature Activation Protocol (SAP). In this way, the signing key is used with a high level of assurance under the sole control of the signatory.

The generation of the digital signature value is carried out within the remote Signature Creation Device (SCDev), while the SSA manages the communication between the system components and provides access to the signing service for authorized signatories.

6 INTERACTION BETWEEN SCASC AND SSASC

The architecture of the remote server signing service includes the interaction between the Signature Creation Application Service Component (SCASC) and the Server Signing Application Service Component (SSASC).

The SCASC receives the documents or their hash values to be signed and prepares the data to be signed. These data are transmitted to the SSASC, which, through the remote Signature Creation Device (SCDev), generates the digital signature value.

The generated signature value is returned to the SCASC, which incorporates it into the relevant electronic signature or electronic seal in accordance with the format used (for example CAdES, PAdES or XAdES).

The SCASC and SSASC may also interact with external trust services, such as a Certification Authority (CA), Registration Authority (RA), certificate status services (OCSP/CRL), Time-Stamping Authority (TSA) and authentication services.

The system also supports batch signing, where multiple documents or document hashes may be signed within a single signing operation.

6.1. Specific requirements for the Signature Creation Application Service Component (SCASC)

BORICA applies the following requirements to the SCASC in accordance with the applicable standards for server-side signing:

The SCASC supports the creation of advanced and qualified electronic signatures (AdES/QES) and the possibility of adding a time-stamp to the signature.

The SCASC supports the creation of electronic signatures in accordance with the applicable electronic signature standards and formats as described in this policy.

The SCASC ensures interaction with the server-side signing component (SSASC) and with the signature creation device (SCDev/QSCD) through secure communication channels.

The SCASC ensures the WYSIWYS principle ("What You See Is What You Sign") by enabling the signatory to review the document, or its representation, before confirming the signing operation.

The architecture of the system permits the participation of external systems or relying parties through secure interfaces, provided that all security and identification requirements set out in this policy are fulfilled.

6.2. Specific requirements for the Server Signing Application Service Component (SSASC)

BORICA AD applies specific requirements in the provision of the remote electronic signature creation service through the Server Signing Application Service Component (SSASC). These requirements ensure the security of the cryptographic operations, the management of the keys, and compliance with the applicable standards and regulatory requirements.

The cryptographic algorithms and key lengths used within the BORICA infrastructure are in compliance with ETSI TS 119 312 and with best security practices for the provision of qualified trust services.

The electronic signature or electronic seal keys of the holders are generated and stored within a protected cryptographic environment (SCDev/QSCD) located within the BORICA infrastructure and compliant with the applicable security standards. The private keys are never exported outside the protected cryptographic module environment.

The server-side signing system uses cryptographic algorithms and hash functions that provide an adequate level of security throughout the full life cycle of the certificates and signatures. Where necessary, BORICA performs periodic reviews of the algorithms used and undertakes updates where a reduced level of security is identified or where changes occur in the applicable legal or standardization requirements.

The management and use of signing keys are performed through a protected server-side signing infrastructure, which ensures that the keys are used only after successful authentication and authorization of the signatory and under sole control, in accordance with Regulation (EU) No 910/2014 (eIDAS).

The policies and practices relating to the provision of the qualified electronic signature and seal service are publicly available to all interested parties through the BORICA website. Documents containing sensitive information, including internal information security procedures, are not published and are accessible only to authorized personnel.

7 GENERATION OF SIGNING KEYS

BORICA AD applies the requirements of the applicable policies and standards for remote electronic signature creation in accordance with Regulation (EU) No 910/2014 (eIDAS) in the generation and management of signing keys.

The signing keys of the users are generated and stored in a Signature Creation Device (SCDev/QSCD) that operates in accordance with its certified configuration.

In the generation and management of signing keys, BORICA AD applies the following requirements:

• Private keys are generated and used exclusively within the SCDev. The device is a certified cryptographic system with a security level of at least Common Criteria EAL4+ or equivalent, compliant with the requirements of EN 419 221.

• Signing keys are generated and stored within the protected environment of the SCDev and cannot be exported from the device, thus ensuring their confidentiality and integrity.

• The cryptographic algorithms and parameters used are compliant with ETSI TS 119 312. BORICA performs periodic reviews of the algorithms used and, where necessary, updates the cryptographic parameters or generates new keys.

• The initialization and management of the SCDev are performed through controlled procedures requiring the participation of at least two authorized operators.

• The cryptographic algorithms used for signature creation are selected so as to ensure an appropriate level of security for the entire validity period of the relevant certificate.

• The signing keys may be generated in advance, independently of the certificate issuance process.

• At SCAL2, the generation and use of the signing keys are managed through a Signature Activation Module (SAM), which ensures that the key is used under the sole control of the signatory. The SAM operates in a protected environment and uses Signature Activation Data (SAD) generated through the Signature Activation Protocol (SAP).

• The remote Signature Creation Device (SCDev) is a cryptographic module operating in a protected environment and allowing the generation and use of signing keys only after successful authentication of the signatory.

8 CREATION OF THE ADES DIGITAL SIGNATURE

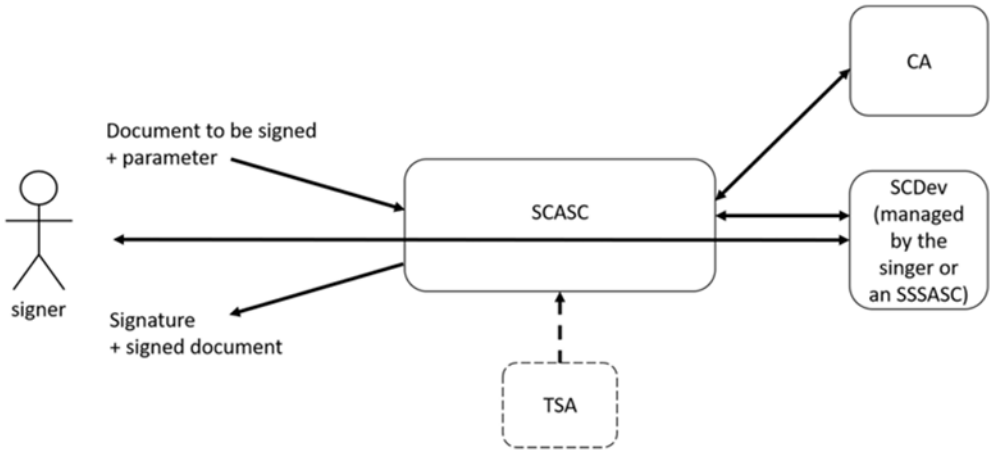
The electronic signature creation process involves the Signature Creation Application Service Component (SCASC). This component receives the document to be signed, or its hash value, together with any additional parameters required for the creation of the signature.

After receipt of the document, the SCASC collects and prepares all information necessary for signing. On this basis, the Data To Be Signed Representation (DTBSR) is formed. This represents the prepared information on which the digital signature value is to be computed. These data are transmitted to the Signature Creation Device (SCDev).

Before the signature is created, the system performs authentication of the signatory and confirmation of the signatory's consent to sign the specific document. Such authentication may be carried out by means of the signing system components or through direct interaction between the signatory and the signature creation device.

Following successful authentication and confirmation of the signing operation, the SCDev uses the signatory's private key and computes the digital signature value. The resulting value is returned to the SCASC, which incorporates it into the final electronic signature applied to the document.

Thus, the SCASC manages the signature creation process, while the SCDev performs the actual cryptographic signing operation using the signatory's private key.



9 FUNCTIONAL MODEL

The Cloud QES platform includes two components:

- a remote server-side component operated and controlled by QTSP BORICA AD;
- a mobile application for smartphones (Android and iOS).

The server-side part of the Cloud QES platform forms part of the B-Trust infrastructure of QTSP BORICA AD and includes two dedicated subsystems:

- Cloud QES Issuance Subsystem;
- Cloud QES Signing Subsystem.

The initial issuance, renewal and management (suspension/reactivation and termination/revocation) of the Cloud QES follow the general functional requirements and the respective procedures for QES described in the

document “B-Trust CPS-eIDAS”. This document contains only the specific features and differences relating to the Cloud QES.

The B-Trust Mobile application is a dedicated application for the Android and iOS mobile platforms for the signatory’s smartphone and serves to activate the creation/generation of the Cloud QES. The B-Trust Mobile application is publicly available for download and is initialized by the signatory on the smartphone.

Within the scope of the B-Trust infrastructure, the server-side part of the Cloud QES platform supports two main functionalities:

• “Registration” and “Issuance” of the Cloud QES – implemented through the Cloud QES Issuance Subsystem;
• “Signing” with the Cloud QES – implemented through the Cloud QES Signing Subsystem.

The “Signing” functionality of the Signing Subsystem uses the following operational components of the B-Trust infrastructure:

- The public register and CRL for qualified certificates (LDAP server);
- OCSP server.

9.1. “Registration” and “Issuance” Functionality of the Cloud QES

The information in this part of the document shall be read together with the relevant information in B-Trust CPS-eIDAS.

The user uses a smart device (smartphone or tablet) with the B-Trust mobile application installed. The process begins with the user’s acceptance of the applicable terms for remote identification and personal data processing, as well as review of the relevant policies and general terms and conditions relating to the provision of qualified trust services.

For registration purposes, the user provides a mobile number and an e-mail address, which are validated by sending a one-time password (OTP). After successful validation, the user captures an image of the identity document, and the system performs automated data extraction through OCR, verification of the document security features, and image quality control.

This is followed by identification through the capture of the user’s face (selfie) and liveness detection, which confirms that the person is real and physically present during the process. The resulting image is compared with the image from the identity document.

The extracted data are validated against available reliable national sources through integration with civil identity registers. Where a match is found, an additional comparison is performed between the registry image, the identity document image and the captured selfie.

The remote identification method is nationally recognized by the competent regulatory authority and forms part of a registered electronic identification service. Following successful completion of the automated checks, the process is also subject to an additional review by an operator of BORICA AD.

9.2 "Management" Functionality of the Cloud QES

The "Management/Maintenance" functionality of the Cloud QES includes:

- temporary suspension of the Cloud QES;
- reactivation of a temporarily suspended Cloud QES;
- termination/revocation of the Cloud QES.

Renewal of the Cloud QES is not supported. **QTSP BORICA AD** issues qualified certificates for Cloud QES with a validity period of **three (3) years**. After expiry of this period, the holder of the Cloud QES may apply for the issuance of a new one.

9.3 "Signing" Functionality of the Cloud QES

Within the scope of the server-side component of the Cloud QES platform, this functionality performs only the generation of the digital signature value (PKCS#1) for the Cloud QES. The generated digital signature and the corresponding certificate for the public signing key are provided to a separate application system, which forms the electronic signature container in accordance with the required format/profile of the electronic signature (CAdES, XAdES, PAdES, ASiCS/E) and the corresponding signature level (BASELINE_B, BASELINE_T, BASELINE_LT, BASELINE_LTA).

9.3.1. Supported Electronic Signature Formats and Levels

AdES Signature Level	Description	CAdES	XAdES	PAdES
Baseline B	Basic electronic signature ensuring the integrity of the signed document and non-repudiation of the signature	CAdES-B-B	XAdES-B-B	PAdES-B-B
Baseline T	Basic signature with an added trusted time-stamp proving the time of signing	CAdES-B-T	XAdES-B-T	PAdES-B-T
Baseline LT	Signature with long-term validation data included (CRL/OCSP) enabling validation of the signed file	CAdES-B-LT	XAdES-B-LT	PAdES-B-LT
Baseline LTA	Signature with long-term validation and archival time-stamps ensuring validity during long-term preservation	CAdES-B-LTA	XAdES-B-LTA	PAdES-B-LTA

Format	Description	Supported Signature Types
CAdES	**Electronic signature format based on CMS/PKCS#7 allowing the signing of arbitrary files and supporting long-term signature validity**	**ENVELOPING, DETACHED**
PAdES	**Electronic signature format for PDF documents where the signature is embedded into the PDF file itself**	**ENVELOPED**

Format	Description	Supported Signature Types
XAdES	Electronic signature format for XML documents supporting extended attributes for long-term validity	ENVELOPED, ENVELOPING, DETACHED

Signature Type	Description
ENVELOPED	The signature is embedded within the signed document
ENVELOPING	The signature contains the signed document
DETACHED	The signature is separate from the signed document

10 PROFILE OF THE CERTIFICATE REVOCATION LIST

10.1. Version

1. The Provider, through its CA, issues, publishes and maintains Certificate Revocation Lists (CRL) in the H.509 v.2 format.
2. The version number is assigned in the issued CRL.

10.2. Format

1. The Provider issues, publishes and maintains a CRL, which format is in accordance with the international guidelines RFC 5280.

CAs of the Provider issue, publish and maintain separate and complete CRLs and record therein only revoked certificates issued by the respective CA.

The Provider does not issue or maintain a scheme of "partial" (delta) CRL, but reserves the right to introduce such a scheme, if necessary.

The main attributes of the CRL are:

- Version;
- Issuer Name - identifies the CA that issued and signed the CRL;
- Effective Date/This update - the time of issue of the CRL;
- Next Update - the period of validity of the CRL. After that period, the CA periodically issues a new list. During the period of validity, in the event of revocation/suspension of a certificate, the CA immediately issues a new CRL;
- Signature algorithm - means the cryptographic mechanism/algorithm for electronic signature of CRL;
- Signature hash algorithm - hash function in the mechanism of the electronic signature.

Additional CRL-attributes are:

- Authority Key Identifier- the identifier of the CA that issues and signs the List. It contains the meaning of "subjectKeyIdentifier" from the certificate of the CA that signs the CRL.

10.3. Format of an Element in the CRL

1. The CRL of the CA contains elements for all certificates revoked by the CA. These elements are constant in the List.

The CRL of the CA contains an element for every certificate suspended by the CA. Such an element in the List is temporary until the resumption of the certificate.

Attributes of the elements in the CRL are as follows:

- "Serial number" - the serial number of a revoked/suspended certificate;

- "Revocation date"- the date of revocation/suspension of the certificate;
- "CRL Reason Code" – code identifying the reason for revocation/suspension.

The meanings of the reason for revocation/suspension of the certificate are as follows:

- "keyCompromise" - compromised private key of the User;
- "CACompromise" - compromised private key of an operational CA of the Provider;
- "affiliationChange" - changed status of a User to another person - changes in the representative authority, revocation of representative authority, termination of employment contract, etc.;
- "superseded" - the certificate is replaced with another;
- "certificateHold" - the certificate is temporarily suspended.

10.4. OCSP Profile

1. The OCSP server of the Provider shall operate and provide the service "online check of certificate status in real time", in accordance with the internationally recognized recommendation IETF RFC 6960.
2. Information of the request profile and response when operating with the OCSP server is available in the above-mentioned technical recommendation, publicly available on the web site of IETF.

11 AUDIT AND CONTROL OF THE PROVIDER'S ACTIVITIES

11.1 Periodic and Event-Driven Review

The supervision of the Provider's legally regulated activities relating to electronic signature certificates and their compliance with the **Electronic Document and Electronic Trust Services Act (ZEDEUU)** and the applicable regulatory framework is carried out by the **Communications Regulation Commission (CRC)** within the scope of its statutory powers.

Internal control over the Provider's activities is assigned by the operational management and/or the Board of Directors of the Provider as a legal entity, and the procedures and scope of such reviews are determined in accordance with the Provider's internal documents.

The management of the Provider performs ongoing operational control over the proper execution of the working instructions by the Provider's personnel.

The management of **BORICA AD** appoints periodic compliance reviews of the current activities against the approved **Practice Statement** and **Policies** applicable to the Provider's activities.

The Provider exercises continuous control over the activities of the **RA/LRA**.

11.2 Qualification of Review Personnel

Review personnel may only be persons who are entitled to perform such functions in accordance with internationally accepted requirements and applicable documents.

The review personnel shall be accredited by an international accreditation body to perform such reviews.

Internal reviews of the activities of the **RA/LRA** are carried out by employees of the Provider authorized for that purpose.

Review personnel may not authorize other persons to perform part or all of the review, except with the explicit consent of the Provider.

Review personnel remain responsible for the facts and circumstances reviewed, regardless of whether they have subcontracted part or all of the review to other persons with the consent of the Provider.

11.3 Relationship of Review Personnel with the Provider

Review personnel shall be independent, shall not be directly or indirectly related to the Provider, and shall have no conflict of interest with the Provider.

The relationship between the Provider and an external review body shall be governed by contract.

11.4 Scope of the Review

The review performed by Conformity Assessment Bodies under **Regulation (EU) No 910/2014**, as amended by **Regulation (EU) 2024/1183**, covers the regulatory requirements applicable to the Provider's activities under **ZEDEUU**.

Internal review may cover any circumstance or activity referred to in this document, including:

- comparison of the practices and procedures set out in this document with their practical implementation in the Provider's operations;
- review of the activities of subcontractors, including external **RA/LRA**;
- other circumstances, facts and activities related to the **B-Trust** infrastructure, at the discretion of the Provider's management.

11.5 Discussion of Results and Actions Following the Review

Based on the assessments made and the review report, the Provider's management defines measures and deadlines for remedying any identified deficiencies and non-conformities.

The Provider's personnel shall take specific actions to eliminate such deficiencies within the prescribed deadlines.

The results of the completed review shall be duly retained in the Provider's archive.

11.6 Term and Termination

The provisions of this document, as well as the Policies for the provision of certificates and trust services associated with it, shall remain valid until the issuance and publication of their subsequent version/revision in the document repository on the Provider's website.

The trust services agreement between the Provider and the User shall remain valid for one year or until the expiry of the validity period of the last certificate issued under the agreement.

Upon termination of the Provider's activities, the provisions, Practice Statement and Policies associated with this document shall cease to apply.

If any individual clause of this document is found to be invalid, the validity of the document as a whole shall remain unaffected and the agreement with the User shall not be impaired. The invalid clause shall be replaced by the applicable mandatory provisions of law.

The trust services agreement between the Provider and the User shall terminate upon the expiry of the validity period of the last certificate issued under the agreement or upon the termination of all certificates issued under the agreement.

The Provider shall securely and properly retain all previous versions of this document and the Policies associated with it.

11.7 Notifications and Communications Between the Parties

The Provider uses statements, letters and notices of the **RA/LRA**, as well as electronic notifications published on its website.

B-Trust customers may send messages, letters, recommendations, questions and complaints to the Provider using the following contact details:

Postal address: 41 Tsar Boris III Blvd., Sofia 1612, Bulgaria
Telephone: 0700 199 10
E-mail: info@b-trust.org
Official website of the Provider: https://www.b-trust.bg

In the event of a complaint, the Provider shall carry out an immediate review and shall send a response to the complainant within **2 business days**.

11.8 Changes to the Document

The Provider may make editorial changes to this document that do not affect the substance of the rights and obligations set out therein.

Changes resulting in a new version/revision of the document shall be published on the Provider's website.

Such changes shall be communicated to the **CRC** and to the interested parties.

Any person may submit proposals for amendments or for the correction of errors by using the Provider's contact details specified above.

11.9 Dispute Resolution and Jurisdiction

Any disputes arising between the parties to the trust services agreement shall be settled by mutual agreement, through understanding and in good faith, and if no such agreement is reached, they shall be resolved by the competent Bulgarian court.

11.10 Governing Law

Any matters not regulated by this document shall be governed by the provisions of Bulgarian law.

11.11 Compliance with Applicable Law

This document has been developed in compliance with **ZEDEUU** and the applicable regulatory framework in force.