InfoNotary

POLICY AND PRACTICE FOR PROVIDING A SERVICE FOR REMOTE SIGNING AND SEALING OF ELECTRONIC DOCUMENTS

OF THE QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

VERSION 1.3

Effective from 30.12.2024 г.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. CONCEPT OF REMOTE ELECTRONIC SIGNATURE/SEAL CREATION (REMOTE SIGNING/SEALING WITH CLOUD-BASED QES). LEGAL COMPLIANCE AND LEGAL EFFECT

Regulation (EU) No 910/2014 regulates the possibility of creating qualified electronic signatures remotely (remote signing) when: **a)** the environment for creating a qualified electronic signature, i.e., the qualified electronic signature creation device, is managed by a Qualified Trust Service Provider on behalf of the Signatory/Creator of the electronic seal; **b)** the cryptographic security requirements for a qualified electronic signature are met during its creation; and **c)** the Signatory/Seal Creator has sole control over the use of their qualified electronic signature/seal creation data, i.e., the data used to activate their private key. A qualified electronic signature/seal created in this way (via a remote signature creation device) meets the requirements of Regulation (EU) No 910/2014 for a qualified electronic signature, which carries the same legal effect as a handwritten signature.

In this context, Infonotary AD (Infonotary/the Provider), as a Qualified Trust Service Provider, offers a service for remote signing/sealing of electronic documents (Remote Signing Service/the Service), in compliance with Regulation (EU) No 910/2014, the applicable European and international standards, and national legislation.

The Provider has implemented and applies specific, secure, and reliable procedures for managing physical and administrative security, uses secure and reliable systems and products, including a trusted environment for remote qualified electronic signature creation, and ensures that this environment is used solely under the control of the Signatory.

1.2. SUBJECT

The main objective of this document, POLICY AND PRACTICE FOR PROVIDING A SERVICE FOR REMOTE SIGNING AND SEALING OF ELECTRONIC DOCUMENTS by the trust service provider INFONOTARY AD (INFONOTARY/the Provider), is to describe and publicly disclose:

- the terms and rules established and applied by INFONOTARY in providing the remote signing/sealing service for electronic documents;
- the applicability and limitations of using the Service
- the specific operational procedures followed by INFONOTARY when providing the Service;
- the means for ensuring the Provider's activities, including their reliability and security, are compliant with the provisions and requirements of Regulation (EU) 910/2014 and the applicable Bulgarian legislation.

This document complements and should be read in conjunction with the latest published versions of the following documents available at: https://www.infonotary.com "Practice for the Provision of Qualified Trust Services", "Policy for the Provision of Qualified Certificate for Qualified Electronic Signature", "Policy for the Provision of Qualified Certificate for Qualified Electronic Seal", "Policy and Practice for the Provision of Remote Video Identification Service" by INFONOTARY PLC . These documents include general terms and requirements for procedures related to identification, issuance, management, and use of qualified certificates for qualified electronic signatures/seals, security requirements, and the generation and storage of key pairs (private and public) for these certificates, as well as their applicability.

In this regard, the text may include, non-exhaustively, references to relevant sections of the aforementioned documents.

This "Policy and Practice for Providing a Service for Remote Signing and Sealing of Electronic Documents" is a public document and may be amended as necessary, with any updates being made publicly accessible to all interested parties at: https://www.infonotary.com .

1.3. COMPLIANCE

This document has been prepared in accordance with the provisions and requirements of the European and national regulatory documents and standards listed below:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, and refers to information regarding the preparation of international recommendations, specifications, and standards in accordance with this Regulation.
- REGULATION (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (Regulation eIDAS 2.0);
- Law on Electronic Document and Electronic Trust Services;
- REGULATION (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;
- CEN EN 419 241-1 „Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements";
- CEN EN 419 241-2 „Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing";
- ETSI TS 119 431-1/2 - Electronic Signatures and Infrastructures (ESI);Policy and security requirements for trust service providers;
- Part 1: TSP service components operating a remote QSCD /SCDev;
- Part 2: TSP service components supporting AdES digital signature creation
- ETSI TS 119 432 - Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
- IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

International standards and specifications are used in their current and valid versions.

2. MAIN PROVISIONS

2.1. TRUST SERVICE PROVIDER

InfoNotary PLC is a Qualified Trust Service Provider in accordance with Regulation (EU) No 910/2014 and has been granted qualified status by the national Supervisory Authority in compliance with the provisions of Regulation (EU) No 910/2014 and national legislation.

InfoNotary PLC is a commercial company registered in the Commercial Register at the Registry Agency under UIC 131276827. The company's registered office and place of business is in Sofia, 16 Ivan Vazov Street. Contact phone: +359 2 9210857; website: http://www.infonotary.com .

The company operates under the registered trademark InfoNotary.

As a qualified provider, InfoNotary PLC performs the following activities and provides the following qualified trust services:

- Issuance and management of qualified certificates for qualified and advanced electronic signatures and seals;
- Issuance and management of qualified website authentication certificates;
- Issuance and management of qualified electronic time stamps;
- Issuance and management of qualified PSD2 certificates;
- Validation services for qualified certificates, qualified electronic signatures and qualified electronic seals, including:
    - Real-time status verification services for qualified certificates issued by InfoNotary (OCSP);
    - Real-time validation services for qualified certificates, qualified electronic signatures, and qualified electronic seals (InfoNotary Qualified Validation Service - IQVS);
- Qualified services for remote signing/sealing of electronic documents;
- Nationally qualified remote video identification service;
- Nationally qualified trust service for electronic identification, including services for issuance and management of electronic identity means, and dynamic electronic identity authentication.

In carrying out its activities and providing qualified trust services, InfoNotary PLC applies its internally implemented Management System, certified according to ISO 9001:2008 and its Information Security Management System, certified according to ISO/IEC 27001:2013.

2.2. DOCUMENT NAMING AND IDENTIFICATION

The document "Policy and Practice for Providing a Service for Remote Signing and Sealing of Electronic Documents" is titled **"InfoNotary Qualified Remote Signing Service (QRSS) CP_CPS"** and is identified by the following Object Identifier (OID): **1.3.6.1.4.1.22144.3.10**, which corresponds to the EU SSASC Policy (OID 0.4.0.19431.1.1.3), in accordance with ETSI TS 119 431-1.

2.3. PARTICIPANTS IN THE REMOTE SIGNING SERVICE

2.3.1. Certification Authority

In accordance with Section 1.3.1 of INFONOTARY's document "Practice for the Provision of Qualified Trust Services."

The operational certification authorities involved in the Service are:

- **InfoNotary Qualified Personal Sign CA** – operational certification authority for issuing qualified certificates for qualified electronic signatures to natural persons;
- **InfoNotary Qualified Legal Person Seal CA** – operational certification authority for issuing qualified electronic seal certificates for legal entities;
- **InfoNotary Device Authentication CA –** operational certification authority for issuing operational authentication certificates for devices

The operational conditions and purposes of the aforementioned certification authorities are in accordance with Sections 1.3.1 and 1.4.1 of the "Practice for the Provision of Qualified Trust Services" and with the respective certification policies of INFONOTARY.

2.3.2. Platform for Cloud Qualified Certificates and Remote Signing and Sealing of Electronic Documents – InfoNotary QRSS

The InfoNotary QRSS platform (the Platform) for cloud-based qualified certificates (Cloud QES/QSeal) and remote signing and sealing of electronic documents provides the following functionalities:

- Generation and secure storage, on behalf of the Signatory/Seal Creator, of an asymmetric key pair (public and private key) through a remote signature/seal creation device – InfoNotary Remote Qualified Signature Creation Device (RQSCD), which is an integral part of the Provider's infrastructure;
- Authentication of the Signatory/Seal Creator to authorize use of the key for signing;
- Verified management and use of cryptographic keys within the RQSCD, solely under the control of the Signatory/Seal Creator for creating a remote electronic signature or remote electronic seal for an electronic document presented in the Platform.

The Platform consists of:

- A remote server system, part of the Provider's infrastructure, including a remote signature creation device (SSA, SAM+HSM). INFONOTARY uses cryptographic modules certified in accordance with the requirements of Regulation 910/2014 (SAM, HSM);
- The InfoNotary SignZone mobile application or a web interface from the Provider's or a third party's information system for activating the Cloud QES/QSeal creation process.

2.3.3. User

A user associated with the signing/sealing key may be:

- A natural person, or a natural person in their capacity as an authorized representative of another individual, a legal entity, or organization, or as the legal representative of a legal entity or organization (Signatory/Seal Creator);
- A device or system operated by or on behalf of a natural or legal person.

The remote signing service may be used by Users who:

- Have downloaded and installed the InfoNotary SignZone mobile application or a third-party mobile app integrated with the InfoNotary Mobile SDK on a smart device under their sole control, or use a web interface from the Provider's or a third party's information system;
- Accept the terms of this document, the Provider's "Practice for Provision of Qualified Trust Services", the General Terms of Use for the application, and the Privacy and Personal Data Protection Policy;
- Use and protect their private and public keys and the access tools for their activation (PINs, passwords, etc.) from compromise, as described in this document and the Provider's "Practice for Provision of Qualified Trust Services".

2.3.4. Relying Parties

A relying party is any natural or legal person/organization that relies on the Provider's remote electronic signature/seal trust services.

Relying parties must have the competence to use electronic signature/seal certificates and should only trust the Provider's issued qualified certificates after verifying their status and validity via the Provider's certificate repositories.

Relying parties can rely on qualified, secure, simple, and convenient automated validation of qualified electronic signatures/seals and the certificates issued by INFONOTARY.

2.3.5. Third Party

A third party is a legal entity, organization, administrative body, or local authority, separate from the Provider, that relies on InfoNotary's trust services and uses the remote signing/sealing service for its own purposes.

Third parties gain access to the remote signing/sealing service after signing an individual agreement with the Provider and integrating with the InfoNotary remote signing and sealing platform.

Third parties must use a valid qualified website authentication certificate (SSL certificate), which will be used for authenticating the third party when using the remote signing/sealing service.

2.4. USE OF CERTIFICATES

2.4.1. Types of Certificates

Under this Policy and Practice, the qualified certificates issued by the Provider for end users (Signatories) related to the Service include: **InfoNotary Qualified Natural Person Signature** - Qualified Certificate for Qualified Electronic Signature (including cloud-based qualified electronic signature) for a natural person; **InfoNotary Qualified Delegated Signature Certificate -** Qualified Certificate for Qualified Electronic Signature with Delegated Authority for a natural person; **InfoNotary Qualified Legal Person Seal -**Qualified Certificate for Qualified Electronic Seal (including cloud-based qualified electronic seal) for a legal entity; Cloud-based qualified certificates for electronic identification – **InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP** for Holders of electronic identification means.

The purpose and operational conditions for the issuance and management of these qualified certificates are in accordance with Sections 3 and 4 of the "Policy for the Provision of Qualified Certificate for Qualified Electronic Signature", the "Policy for the Provision of Qualified Certificate for Qualified Electronic Seal", and Sections 1.4.1.2.1, 3, and 4 of the "Practice for the Provision of Qualified Trust Services" of INFONOTARY.

To ensure the security and reliability of functionalities and services provided remotely (via the InfoNotary SignZone mobile application, the Provider's web interface, or integrated systems, mobile apps, or third-party web portals), the Provider introduces the use of: Qualified Website Authentication Certificate, and Qualified Mobile Device Authentication Certificate – **InfoNotary Mobile Device Authentication Certificate**.

The **InfoNotary Mobile Device Authentication Certificate** is issued to an authenticated User with the InfoNotary SignZone mobile application installed. The certificate is issued to a natural person, the owner/user of a mobile device with a unique identifier, which is embedded in the certificate and can be used to authenticate the mobile device to information systems, internet applications, for performing secure and encrypted communication, and for ensuring the origin of electronic data and information accessible through the InfoNotary SignZone mobile application provided by the Provider. The qualified certificate may also include specific attributes that provide the necessary information for identifying the device.

2.4.2. Applicability, Use, and Accessibility of the Remote Signing/Sealing Service for Electronic Documents

The service may be used by users (natural persons either in their own capacity or as legal/authorized representatives of a legal entity) who are Signatory/Creators of a valid cloud-based qualified certificate for a qualified electronic signature/seal (Cloud QES/ Cloud QESeal) issued and maintained by INFONOTARY PLC.

The remote signing service can be accessed via the Provider's mobile application – InfoNotary SignZone, or through a web interface of an information system of the Provider or a third party (e.g., financial or insurance institutions) that has entered into an agreement with INFONOTARY and has integrated with the Provider's InfoNotary QRSS.

Where practically feasible, the Provider ensures the service is accessible to people with disabilities. Accessibility is provided without compromising or excluding compliance with security requirements, applicability, or conformance with Regulation (EU) No 910/2014, national legislation, and the internal policies and procedures of the Provider.

2.4.3. Limitations of the Certification Function

The remote signing service must not be used in a manner that violates the confidentiality and security of personal data.

The Provider shall not be held liable for damages arising from:

- use of the remote signing service outside the permitted scope and application limitations related to its intended use, which will result in the invalidation of any guarantees given by INFONOTARY to users and relying parties;
- accidental events of force majeure, including malicious actions by third parties.

2.5. MANAGEMENT OF THE PROVIDER'S CERTIFICATION POLICY

The Provider's "Policy and Practice for Providing a Service for Remote Signing and Sealing of

Electronic Documents" is established by the Board of Directors of INFONOTARY PLC.

All changes, revisions, and additions to this Policy are adopted by the Board of Directors of INFONOTARY PLC.

New versions of the document are published upon approval in the Provider's Document Register, which is publicly accessible at: https://www.infonotary.com

All comments, inquiries for information, and requests for clarification regarding this Policy may be sent to the following address: INFONOTARY PLC, 1000 Sofia, Bulgaria, 16, Ivan Vazov"str., e-mail: legal@InfoNotary.com

2.6. TERMS AND ABBREVIATIONS

Qualified Trust Service Provider	A trust service provider that provides one or more qualified trust services and has been granted qualified status by a supervisory authority.
Service Provider using Server-Side Signing Application/Remote Signing (SSASP)	A qualified trust service provider managing a component of the server-side signing/remote signing application
Persons Identification Data	A set of data that enables the identification of a natural or legal person, or a natural person representing a legal entity.
Electronic Signature Creation Data	Unique data used by the electronic signature Holder to create an electronic signature.
Relying Party	A natural or legal person that relies on electronic identification or a trust service.
Trusted Source	Any source, regardless of its form, that can be relied upon to provide accurate data, information, and/or evidence/facts that can be used to verify identity.
Electronic Identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
Electronic Identity	A set of attributes recorded in electronic form, based on which a person can be uniquely distinguished from other individuals in a virtual environment, for the purpose of granting access to information systems or enabling the performance of electronic statements.
Applicant/User	A person (legal or natural) whose identity needs to be verified.

Qualified Trust Service

A trust service that meets the applicable requirements set out in Regulation (EU) No. 910/2014.

Server-Side Signature Service Component (SSASC)

A component of the Provider's service that uses a server-side signing application to generate a digital signature value on behalf of the signer.

Signature Activation Module (SAM)

A secure software element located in a protected, access-controlled environment within the Provider’s infrastructure, which ensures the sole control of the Signatory over the use of the electronic signature/seal creation data when using the remote signing service, and which complies with the requirements of Regulation (EU) No. 910/2014.

Remote Signature Creation Device

A signature creation device used remotely from the signatory’s perspective, which ensures control over the signing operation on behalf of the signatory.

Remote Video Identification / Onboarding

An identity verification process in which the applicant/user is physically distant from the location where the identity verification is being carried out.

Platform for Cloud-Based Qualified Certificates and Remote Signing and Sealing of Electronic Documents

A dedicated part of the Provider’s trust service infrastructure that meets the requirements set out in Annex II of Regulation (EU) No. 910/2014. It is used for the generation, storage, and management of data for the creation of cloud-based qualified electronic signatures/seals by the Provider, on behalf of the Signatory or the Creator of the electronic seal.

Regulation

REGULATION (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

eIDAS 2.0 Regulation

REGULATION (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

GDPR Regulation

REGULATION (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

Digital Signature Value

The result of a cryptographic transformation of a data unit that protects it against forgery and enables the recipient of the data unit to verify its origin and integrity.

Electronic Identification Means

A material and/or immaterial unit containing person identification data and which is used for authentication for an online service

Electronic Seal Creator

A legal entity that creates electronic seals and is listed in the electronic seal certificate as the creator.

Reference to Electronic Identification Means

Data used in the SSASC (Server Signing Application Service Component) as a reference to the electronic identification means for authenticating the signatory.

Electronic Signature Holder/Signatory

A natural person who creates an electronic signature.

Third Party

An entity that relies on the trust services provided by InfoNotary AD and uses the remote signing/sealing service of electronic documents for its own purposes.

Trust Service

An electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;

Qualified Electronic Signature Creation Device (SCDev)

A configured software or hardware device used for the creation of an electronic signature, which complies with the requirements set out in Annex II of Regulation (EU) No 910/2014.

Remote Qualified Signature/Seal Creation Device (RQSCD)

A signature/seal creation device that complies with the requirements set out in Annex II of Regulation (EU) No 910/2014, forming a dedicated part of the provider's infrastructure, used remotely from the signer's perspective and ensuring control over the signing operation on behalf of the signer

Cloud-Based Qualified Electronic Signature/Seal Certificate

A qualified electronic signature certificate issued by a qualified trust service provider to a remote qualified signature/seal creation device.

ABBREVIATIONS

TSP	Trust service provider
CP	Certificate Policy
CPS	Certification Practice Statement
ETSI	European Telecommunications Standards Institute
EU	European Union
ISO	International Standardization Organization
OID	Object Identifier
PKI	Public Key Infrastructure
eID	Electronic Iaentification
EUSCP	EU SSASC Policy
NCP	Normalized Certificate Policy
NSCP	Normalized SSASC Policy
SCDev	Signature Creation Device
SCP	SSASC Policy
SSASC	Server Signing Application Service Component
SSASP	Server Signing Application Service Provider
QSCD	Qualified electronic Signature/Seal Creation Device

3. OBLIGATIONS FOR PUBLICATION AND MAINTENANCE OF REGISTERS

In accordance with item 2 of the INFO-NOTARY document "Practice for Providing Qualified Certification Services."

4. IDENTIFICATION AND AUTHENTICATION

During initial identification and verification of identity, users who are Holders of cloud qualified certificates as specified in section 2.4.1, the Provider shall follow the rules and conditions set forth in item 3 of the document "Practice for Providing Qualified Certification Services" and item 4.2.1 of the document Policy and Practice for Providing Remote Video Identification Service of INFONOTARY.

5. OPERATIONAL CONDITIONS

Operational activities for providing the Remote Signing/Sealing Service include: providing access to download the mobile application InfoNotary SignZone, authenticating the User (Holder/Seal Creator) to activate the private key for creating a qualified electronic signature/seal, creating a qualified electronic signature remotely upon request of the Holder/Seal Creator.

The Provider applies the operational rules and procedures for issuing and managing cloud qualified certificates under section 2.4.1, which are defined in item 3 of the INFONOTARY document "Practice for Providing Qualified Certification Services." This document specifies conditions regarding the issuance and management of the qualified certificate for mobile device authentication InfoNotary Mobile Device Authentication Certificate.

5.1. DOWNLOAD OF THE INFONOTARY SIGNZONE MOBILE APPLICATION

The InfoNotary SignZone mobile application is published in the App Store and Google Play electronic stores and depending on the operating system of the User's smart device, it can be downloaded and installed.

5.2. ISSUANCE OF THE QUALIFIED CERTIFICATE FOR MOBILE DEVICE AUTHENTICATION

5.2.1. Actions of the certification authority upon issuing the Certificate

The operational certification authority InfoNotary **Device Authentication CA** of the Provider issues the certificate based on a request received from the Registration Authority.

The Provider issues the **InfoNotary Mobile Device Authentication Certificate** to each User with the InfoNotary SignZone mobile application installed, whose identity has been successfully verified through remote video identification, according to section 4.2 of the "Policy and Practice for Providing Remote Video Identification" document.

5.3. ACCEPTANCE AND PUBLICATION OF THE CERTIFICATE

5.3.1. Acceptance of the certificate

The qualified certificate for mobile device authentication contains a specific identifier and attributes related to the User's mobile device. In this respect, the certificate is not subject to acceptance by the User.

5.3.2. Publication of the certificate

In accordance with item 4.4.2 of the INFONOTARY document "Practice for Providing Qualified Certification Services."

5.4. RENEWAL OF THE CERTIFICATE

Not supported by the Provider.

5.5. KEY REPLACEMENT IN THE CERTIFICATE AND CERTIFICATE MODIFICATION

Not supported by the Provider.

5.6. TERMINATION OF THE CERTIFICATE

The qualified certificate for mobile device authentication is terminated:

- Upon request by the Holder by deleting/deactivating the user profile or terminating the Contract for the Remote Signing Service.
- Upon each new remote video identification process performed by the User.
- Upon termination of the legal entity of the Provider of qualified certification services.

5.6.1. Period within which the Certification Authority should process the termination request

In accordance with item 4.9.4 of the INFONOTARY document "Practice for Providing Qualified Certification Services."

5.6.2. Certificates Revocation List

In accordance with items 4.9.6, 4.9.7, and 4.9.8 of the INFONOTARY document "Practice for Providing Qualified Certification Services."

5.6.3. SUSPENSION AND REINSTATEMENT OF THE CERTIFICATE

Not supported by the Provider.

6. REMOTE SIGNING SERVICE

6.1. GENERAL CHARACTERISTICS AND DESCRIPTION

The remote signing service provided by INFONOTARY is implemented through the **InfoNotary QRSS Platform** (the Platform), which complies with the security requirements of the EN 419 241-1 standard and ensures that the signing/sealing key of the Holder/Seal Creator is used solely and exclusively under their control and for its intended purpose

INFONOTARY, in accordance with ETSI TS 119 432, has implemented the so-called SCAL 2 architecture of the remote signing service, which provides a high level of security assurance by enabling personal control over the use of signing/sealing keys through the use of a Signature Activation Module (SAM).

The overall scheme of components, interfaces, and protocols providing the specific functionalities as part of the process for creating remote qualified electronic signatures/seals used by INFONOTARY in the service implementation is presented in Figure 1.

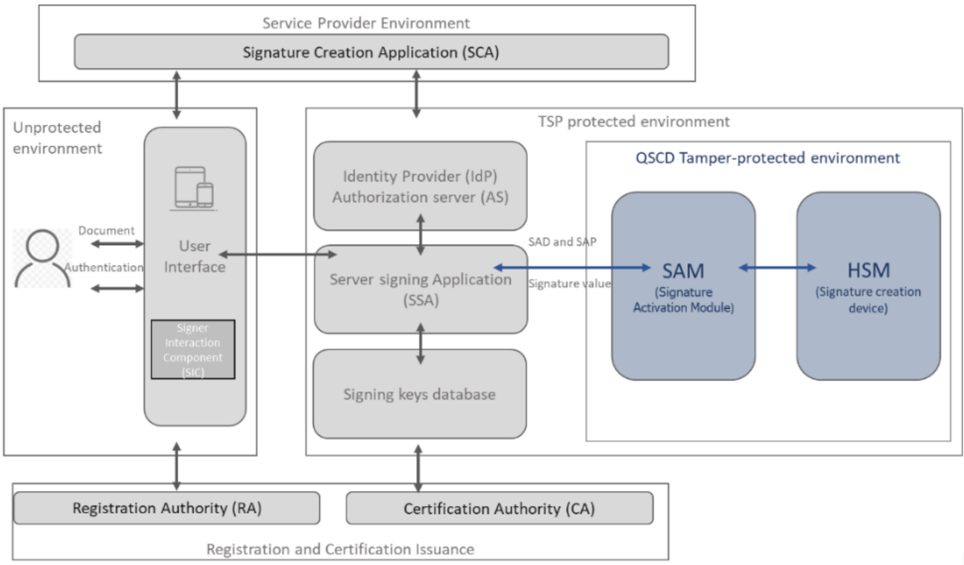
Service Provider Environment
Signature Creation Application (SCA)
Unprotected environment
Document
Authentication
User Interface
Signer Interaction Component (SIC)
TSP protected environment
Identity Provider (IdP) Authorization server (AS)
Server signing Application (SSA)
Signing keys database
SAD and SAP
Signature value
QSCD Tamper-protected environment
SAM
(Signature Activation Module)
HSM
(Signature creation device)
Registration Authority (RA)
Certification Authority (CA)
Registration and Certification Issuance

Fig. 1

The diagram shows the interaction of the main components SCA and SSA with other elements involved in the remote signing process. The SCA consists of a signing application and a remote signature creation device. The SCA uses the remote signature creation device to generate, maintain, and use the signing keys under the control of their Holders/Seal Creators. The SCA is the component responsible for generating the signature. The SCA sends a signature creation request to the SSA.

In this implementation model, the Provider's secure environment is complemented by the so-called tamper-protected environment (QSCD Tamper-protected environment). It protects the use of signing/sealing keys and manages the activation of the signature/seal, ensuring it is solely under the control of the Holder/Seal Creator. This is realized by the SAM module, which ensures the security, confidentiality, and integrity of the signing/sealing key that can be activated by the SCA. The SAM verifies the signature activation data to identify the Holder/Seal Creator and to obtain their permission to activate the signing/sealing key. Upon successful identification of the Holder/Seal Creator, the corresponding key can be used to sign/seal on behalf of the Holder within a defined time period and/or a defined number of signatures. This process provides a high level of security, ensuring that signing keys are controlled solely by the Holder. The signature activation data is transmitted in a protected form directly from the personal device (PC, smartphone, tablet, etc.) of the signer to the SAM through a secure/protected channel to guarantee the personal control of the Holder/Seal Creator over the signing/sealing key and prevent misuse of this key

The CA/RA, OCSP and CRL, Time Stamp, authentication, and authorization services are external to the service.

6.2. FUNCTIONAL MODEL FOR SIGNATURE CREATION

The purpose of the Service is to create a qualified remote electronic signature/seal, which covers: a) the document/data to be sent and signed by the User (signer), b) the certificate with which the signing is performed, and c) attributes supporting the signature, its validation, and purpose. The functional model of the remote signature creation environment used by the Provider consists of:

- A User who wants to create a signature/seal;
- A mobile device — under the control of the Holder/Seal Creator and an active mobile

phone number capable of receiving short text messages (SMS);

- A management application, which represents the environment (e.g., mobile app, information system) the signer uses to access the signing functionality; and
- The InfoNotary QRSS Platform, which implements the signing functionality.

The qualified remote signing service allows the creation of the following signature formats and profiles:

Format/Profile	**BASELINE_B**	**BASELINE_T**	**BASELINE_LT**	**BASELINE_LTA**
XAdES	√	√	√	√
PAdES	√	√	√	√
ASiCS/ ASiCE	√	√	√	√
JadES	√	√	√	√

6.3. ACTIVATION OF THE REMOTE SIGNING SERVICE

The activation of the Remote Signing Service takes place immediately after the issuance of the qualified cloud certificate for electronic signature/seal.

In order to use the Remote Signing Service, the Holder/Seal Creator must have installed the InfoNotary Mobile application and created a PIN for access and signing with the private key linked to a valid qualified cloud certificate for electronic signature/seal.

6.4. USE OF THE REMOTE SIGNING SERVICE

The procedure for creating remote signing/sealing of electronic documents is as follows:

- The Holder/Seal Creator launches the mobile application and enters their access code (PIN);
- The Holder/Seal Creator uploads documents for signing/sends a request to sign an electronic document to the InfoNotary Platform;
- The Holder/Seal Creator reviews the documents available in the Platform for signing, addressed to them and sent for signing by a third party through the Platform;
- After verifying the correctness of the access code (PIN), all requests for creating electronic signatures/documents are downloaded/viewed in the application;
- The Holder/Seal Creator may review the document(s) within the application;
- If the Holder/Seal Creator decides to sign the corresponding documents, they press the "Sign" button and enter their personal access code/private key activation code;
- If the Holder/Seal Creator has entered the correct personal access/private key activation code, then using the private key stored in the secure cryptographic device RQSCD, the Provider creates the respective qualified electronic signature and returns/displays the signed document in the mobile application.

When the Remote Signing Service is used by a third party integrated with the Provider's

Platform, it sends a request to sign an electronic document to the InfoNotary Platform. Part of the data contained in the request includes identification data of the Holder/Seal Creator who must sign the document, as well as the document itself or its hash value, among other data.

The Provider notifies the Holder/Seal Creator that there are pending documents for signing. To perform the signing, the Holder/Seal Creator follows the steps described above.

7. CONTROL OF EQUIPMENT, PROCEDURES AND MANAGEMENT

The Remote Signing Service is performed by the Provider’s Cloud Qualified Certificates and Remote Signing and Sealing Platform, which is a functional part of the Provider’s PKI infrastructure built and audited in accordance with the Regulation’s requirements, used to provide qualified certification services. In this regard, the rules and procedures described in the INFONOTARY document "Practice in Providing Qualified Certification Services" are applied for managing and operational control of equipment, security, and its activity. This document supplements some of these rules and procedures where applicable.

7.1. PHYSICAL CONTROL

In accordance with section 5.1 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.1. Location and construction of premises

In accordance with section 5.1.1 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.2. Physical access

In accordance with section 5.1.2 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.3. Power supply and climatic conditions

In accordance with section 5.1.3 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.4. Flooding

In accordance with section 5.1.4 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.5. Fire alarm and protection

In accordance with section 5.1.5 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.6. Data storage

In accordance with section 5.1.6 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.7. Decommissioning of technical components

In accordance with section 5.1.7 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.8. Component redundancy

In accordance with section 5.1.8 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2. PROCEDURAL CONTROL

In accordance with section 5.2 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2.1. Positions and functions

In accordance with section 5.2.1 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2.2. Number of personnel per task

In accordance with section 5.2.2 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2.3. Identification and authentication for each position

In accordance with section 5.2.3 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2.4. Requirements for separation of duties for different functions

In accordance with section 5.2.4 of the INFONOTARY document Certification practice statement for qualified certification services".

7.3. PERSONNEL CONTROL, QUALIFICATION, AND TRAINING

In accordance with section 5.3 of the INFONOTARY document Certification practice statement for qualified certification services".

7.3.1. Requirements for independent suppliers

In accordance with section 5.3.1 of the INFONOTARY document Certification practice statement for qualified certification services".

7.3.2. Documentation provided to employees

In accordance with section 5.3.2 of the INFONOTARY document Certification practice statement for qualified certification services".

7.4. PROCEDURES FOR CREATING AND MAINTAINING LOGS OF INSPECTIONS

In accordance with section 5.4 of the INFONOTARY document Certification practice statement for qualified certification services".

7.4.1. Frequency of record creation

In accordance with section 5.4.1 of the INFONOTARY document Certification practice statement for qualified certification services".

7.4.2. Retention period of records

In accordance with section 5.4.2 of the INFONOTARY document Certification practice statement for qualified certification services".

7.4.3. Protection of records

In accordance with section 5.4.3 of the INFONOTARY document Certification practice statement for qualified certification services".

7.4.4. Procedure for creating backups of records

In accordance with section 5.4.4 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5. ARCHIVE

In accordance with section 5.5 of the INFONOTARY document Certification practice statement for qualified certification services".

Additionally, the Provider keeps as an internal archive the evidence from the authenticity verification process, in a manner that: prevents forgery and alteration; guarantees confidentiality of information; and ensures the ability to search, retrieve, and verify.

7.5.1. Types of archives

In accordance with section 5.5.1 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5.2. Retention period

In accordance with section 5.5.2 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5.3. Archive protection

In accordance with section 5.5.3 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5.4. Archive recovery procedures

In accordance with section 5.5.4 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5.5. Requirements for date and time stamping of records

In accordance with section 5.5.5 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5.6. Archive storage

In accordance with section 5.5.6 of the INFONOTARY document Certification practice statement for qualified certification services".

7.5.7. Procedures for obtaining and verifying archive information

In accordance with section 5.5.7 of the INFONOTARY document Certification practice statement for qualified certification services".

7.6. CERTIFICATE KEY CHANGE

In accordance with section 5.6 of the INFONOTARY document Certification practice statement for qualified certification services".

7.7. KEY COMPROMISE AND RECOVERY AFTER DISASTERS AND UNFORESEEN EVENTS

In accordance with section 5.7.1 and 5.7.2. of the INFONOTARY document Certification practice statement for qualified certification services".

7.8. PROCEDURES FOR TERMINATION OF PROVIDER'S ACTIVITIES

7.9. Termination of activities

In accordance with section 5.8.1 of the INFONOTARY document Certification practice statement for qualified certification services".

7.9.1. Transfer of activities to another qualified provider of qualified certification services

In accordance with section 5.8.2 of the INFONOTARY document Certification practice statement for qualified certification services".

7.9.2. Revocation of the Provider's qualified status

In accordance with section 5.8.2 of the INFONOTARY document Certification practice statement for qualified certification services".

8. TECHNICAL SECURITY CONTROL

8.1. GENERATION AND INSTALLATION OF KEY PAIRS

In accordance with section 6.1 of the INFONOTARY document Certification practice statement for qualified certification services".

8.1.1. Key pair generation

8.1.1.1. Generation of the Provider's Certification Authority private key

In accordance with section 6.1.1.1 of the INFONOTARY document Certification practice statement for qualified certification services".

8.1.2. Generation of Subscriber key pairs

In accordance with section 6.1.1.2 of the INFONOTARY document Certification practice statement for qualified certification services".

The Provider always generates the key pair of the Holder/Seal Creator after successful identification and confirmation of their identity.

Each generated key pair is uniquely linked to the certified client profile of the Holder/Seal Creator used in the Remote Signing Service.

When the Provider generates the key pair on behalf of the Holder/Seal Creator, the private key is generated and stored in encrypted form in the Provider's RQSCD, and access is controlled by a personal access code (PIN), password, or key under the Holder/Seal Creator's control.

The private key of a cloud certificate for qualified electronic signature/seal is remotely accessible and can only be activated by the Holder/Seal Creator using a personal access code (PIN), password, or key under their control.

8.1.3. Delivery of the private key

In accordance with section 6.1.2 of the INFONOTARY document Certification practice statement for qualified certification services".

8.1.4. Delivery of the public key

In accordance with section 6.1.4 of the INFONOTARY document Certification practice statement for qualified certification services".

8.1.5. Key length

In accordance with section 6.1.5 of the INFONOTARY document Certification practice statement for qualified certification services".

8.2. PROTECTION OF THE PRIVATE KEY AND TECHNICAL CONTROL OF THE CRYPTOGRAPHIC MODULE

8.2.1. Cryptographic module standards

In accordance with section 6.2.1 of the INFONOTARY document Certification practice statement for qualified certification services".

8.2.2. Control of private key storage and use

In accordance with section 6.2.2 of the INFONOTARY document Certification practice statement for qualified certification services".

8.2.3. Storage of private keys

In accordance with section 6.2.3 of the INFONOTARY document Certification practice statement for qualified certification services".

8.2.4. Archiving of private keys

In accordance with section 6.2.4 of the INFONOTARY document Certification practice statement for qualified certification services".

8.2.5. Transfer of private keys into and out of the cryptographic module

In accordance with section 6.2.4 of the INFONOTARY document Certification practice statement for qualified certification services".

8.2.6. Activation and Deactivation of Private Keys

In accordance with section 6.2.6 of the INFONOTARY document Certification practice statement for qualified certification services".

Additionally, the creation of remote qualified electronic signatures/seals requires the identification and authentication of the Holder/Seal Creator for the purpose of activating their issued cloud certificate and the corresponding private key.

The authentication of the Holder/Seal Creator is performed through their two-factor authentication on the Platform via the InfoNotary Mobile application: a) possession of a unique mobile device with an activated user profile in the InfoNotary Mobile application, validated by the issued authentication certificate on the mobile device, and b) validation of a personal identification code (PIN) created by and known only to the Holder/Seal Creator.

The verification and confirmation of these attributes are carried out by the components specified in item 6.1 (fig. 1), the Identity Provider and SAM, within the InfoNotary QRSS.

Upon successful authentication of the Holder/Seal Creator, the Provider activates the private key of the Holder/Seal Creator to perform the specific cryptographic operation, i.e., remote creation of qualified electronic signatures/seals/remote signing/sealing of an electronic document as commissioned by the Holder/Seal Creator.

In case of unsuccessful authentication of the Holder/Seal Creator, the Provider refuses to perform the respective cryptographic operation.

The Provider always verifies the validity of the respective cloud certificate before using the private key and refuses to use a key for a cloud qualified certificate that has expired.

The private key of the Holder of a cloud certificate for electronic signature is automatically deactivated after performing the cryptographic operation (remote signing of the electronic document) for which it was activated, and by terminating logical access to the protected user profile in the RQSCD of the cloud signing platform.

8.2.7. Destruction of Private Keys

A private key of a Holder of a cloud certificate for electronic signature is destroyed by deleting it from the protected user profile in the RQSCD on the InfoNotary QRSS, in the following cases:

Expiration of the validity period of the issued cloud certificate for qualified electronic signature/seal;

Termination of the issued cloud certificate for qualified electronic signature/seal;

Termination of the contract for providing certification services;

A request submitted by the Holder/Seal Creator or deletion of the client profile in the Provider's systems;

Termination/destruction of the logical path/access between the management application (e.g., mobile app, information system) and the protected user profile in the RQSCD on the cloud signing platform.

8.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

8.3.1. Archiving of the Public Key

In accordance with section 6.3.1 of the INFONOTARY document Certification practice statement for qualified certification services".

8.3.2. Certificate Validity Period and Key Pair Usage Period

In accordance with section 6.3.2 of the INFONOTARY document Certification practice statement for qualified certification services".

8.4. ACTIVATION DATA

In accordance with section 6.4 of the INFONOTARY document Certification practice statement for qualified certification services".

8.5. COMPUTER SECURITY CONTROL

In accordance with section 6.5 of the INFONOTARY document Certification practice statement for qualified certification services".

8.6. TECHNICAL CONTROL AND LIFECYCLE

In accordance with section 6.6 of the INFONOTARY document Certification practice statement for qualified certification services".

8.7. NETWORK SECURITY CONTROL

In accordance with section 6.7 of the INFONOTARY document Certification practice statement for qualified certification services".

9. CERTIFICATE PROFILES

9.1. Certificate Profile for InfoNotary Mobile Device Authentication CP

InfoNotary Mobile Device Authentication Certificate		
Basic x509 Attributes:		
Attribute		Value
Version		3 (0x02)
Serial number;		Unique to the Provider's Register from 8 to 16-byte number
Valid from		Date and time of signing
Valid to		Date and time of signing + 5 years
Signature Algorithm		SHA256/RSA
Issuer:		
Attribute		Value
Domain Component	DC	deviceauth-ca
Common Name	CN	InfoNotary Device Authentication CA
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	TSP CA
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Common Name	CN	Unique mobile device ID

Domain Component	DC	deviceauth-ca
Organizational Unit Name	OU	*optional
Additional attributes of x509 extensions (x509v3 extensions):		
Attribute	Value	
Basic Constraints (Critical)	End entity	
Key Usage (Critical)	Digital Signature, Key Encipherment, Key agreement	
Public Key	RSA 2048 bits, ECDSA 256	
Authority Key Identifier	AuthorityKeyIdentifier	
Subject Key Identifier	SubjectKeyIdentifier	
Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://repository.InfoNotary.com/device-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.InfoNotary.com/qualified	
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.InfoNotary.com/crl/deviceauth-ca.crl	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.9.1 Qualifier: Notice Text= InfoNotary Mobile Device Authentication Certificate	
Extended Key Usage (Non Critical)	Client Authentication3	

10. MONITORING AND CONTROL OF ACTIVITIES

In accordance with section 8 of the INFONOTARY document Certification practice statement for qualified certification services‟.

10.1. REGULAR OR EXTRAORDINARY AUDIT

In accordance with section 8.1 of the INFONOTARY document Certification practice statement for qualified certification services‟.

10.2. QUALIFICATION OF AUDITORS

In accordance with section 8.2 of the INFONOTARY document Certification practice statement for qualified certification services".

10.3. RELATIONSHIP BETWEEN AUDITORS AND THE ORGANIZATION BEING AUDITED

In accordance with section 8.3 of the INFONOTARY document Certification practice statement for qualified certification services".

10.4. SCOPE OF THE AUDIT

In accordance with section 8.4 of the INFONOTARY document Certification practice statement for qualified certification services".

10.5. TAKING ACTIONS TO CORRECT DEFICIENCIES

In accordance with section 8.5 of the INFONOTARY document Certification practice statement for qualified certification services".

11. OTHER BUSINESS AND LEGAL TERMS

11.1. PRICES AND FEES

In accordance with section 9.1 of the INFONOTARY document Certification practice statement for qualified certification services".

11.1.1. Remuneration under the Contract for Qualified Certification Services

In accordance with section 9.1.1 of the INFONOTARY document Certification practice statement for qualified certification services".

11.1.2. Invoicing

In accordance with section 9.1.2 of the INFONOTARY document Certification practice statement for qualified certification services".

11.1.3. Policy for Certificate Return and Refund

In accordance with section 9.1.3 of the INFONOTARY document Certification practice statement for qualified certification services".

11.2. FINANCIAL RESPONSIBILITIES

In accordance with section 9.2.1 of the INFONOTARY document Certification practice statement for qualified certification services".

11.3. INSURANCE OF ACTIVITY

In accordance with section 9.2.2 of the INFONOTARY document Certification practice statement for qualified certification services".

11.4. INSURANCE COVERAGE FOR END USERS

In accordance with section 9.2.3 of the INFONOTARY document Certification practice statement for qualified certification services".

The insurance does not cover and the Provider is not liable for damages resulting from:

- Failure to comply with the obligations of Users/Trusting Parties/Third Parties related to the remote signing service arising from this document, the Provider's practice for qualified certification services, the General Terms of Use of the InfoNotary SignZone application, and the individual contract;
- Loss of mobile device or compromise of the secret code (PIN) for application access by the user due to negligence in safeguarding or using it;
- Malicious acts by third parties (hacker attacks, device theft, unauthorized access, etc.);
- Illegal actions by Users and Trusting/Third Parties;
- Force majeure, accidents, and other events beyond the Provider's control.

11.5. CONFIDENTIALITY OF INFORMATION

In accordance with section 9.3 of the INFONOTARY document Certification practice statement for qualified certification services".

11.5.1. Scope of Confidential Information

In accordance with section 9.3.1 of the INFONOTARY document Certification practice statement for qualified certification services".

Additionally, the Provider considers confidential information any documents sent for signing or signed through SignZone and data used for addressing electronic documents sent via SignZone.

11.5.2. Information Outside the Scope of Confidential Information

In accordance with section 9.3.2 of the INFONOTARY document Certification practice statement for qualified certification services".

11.5.3. Obligation to Protect Confidential Information

In accordance with section 9.3.3 of the INFONOTARY document Certification practice statement for qualified certification services".

11.6. PERSONAL DATA PRIVACY

In accordance with section 9.4 of the INFONOTARY document Certification practice statement for qualified certification services".

11.7. INTELLECTUAL PROPERTY RIGHTS

In accordance with section 9.5 of the INFONOTARY document Certification practice statement for qualified certification services".

11.8. OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES

In accordance with section 9.6 of the INFONOTARY document Certification practice statement for qualified certification services".

11.8.1. Provider's Obligations, Responsibilities, and Warranties

In accordance with section 9.6.1 of the INFONOTARY document Certification practice statement for qualified certification services".

11.8.2. Guarantees and Responsibility of the Registration Authority

In accordance with section 9.6.2 of the INFONOTARY document Certification practice statement for qualified certification services".

11.8.3. Obligations and Responsibilities of Users of the Remote Signing/Sealing Service

In accordance with section 9.6.3 of the INFONOTARY document Certification practice statement for qualified certification services".

Additionally, when using the Remote Signing/Sealing Service, the User undertakes the following obligations and responsibilities:

- To comply with the conditions of this document, the Provider's practice for qualified certification services, the General Terms of Use of the Mobile Application, and the Privacy and Personal Data Protection Policy;
- To provide truthful, accurate, and complete information requested by the Provider, in accordance with regulatory requirements and applicable Policies and Practices;
- Not to make false statements or submit forged documents to the Registration Authority relevant to the service;
- To strictly follow the security requirements established by the Provider;
- To keep the created secret code (PIN) confidential and prevent unauthorized use;
- To promptly request suspension or termination of access to the mobile application from the Provider if the PIN is compromised, misused, or at risk of misuse.

The User is liable to INFONOTARY for any failure to meet these obligations arising from this document, the Provider's practice, the General Terms of Use, with the Provider holding the User responsible for damages.

11.8.4. Obligations and Responsibilities of Trusting Parties/Third Parties

Obligations, responsibilities, and the integration method of Trusting Parties/Third Parties with INFONOTARY's remote signing platform are governed by the individual contract with the Provider.

11.9. DISCLAIMER

In accordance with section 9.7 of the INFONOTARY document Certification practice statement for qualified certification services".

INFONOTARY is not liable for damages caused by:

- Failure of Users of the Remote Signing Service to fulfill obligations under this document, the Provider's practice, and the General Terms of Use of InfoNotary SignZone;
- Loss of mobile device or compromise of the secret code (PIN) due to negligence;
- Malicious acts by third parties (hacker attacks, theft, unauthorized access, etc.);
- Illegal actions by Users and Trusting/Third Parties;
- Force majeure, accidents, and other events beyond the Provider's control.

The Provider is not liable for damages to Trusting/Third Parties resulting from failure to fulfill obligations or negligence as defined in the signed contract.

11.10. LIMITATION OF LIABILITY

In accordance with section 9.8 of the INFONOTARY document "Certification practice statement for qualified certification services".

11.11. COMPENSATIONS TO THE PROVIDER

In all cases of failure by Users of the Remote Signing Service or Trusting/Third Parties to fulfill obligations arising from this document, the Provider's Certification practice statement for qualified certification services, and the General Terms of Use of mobile application, the Provider will hold Users and Trusting/Third Parties responsible for damages.

11.12. TERM AND TERMINATION

11.12.1. Term

This "Policy and Practice for Providing Qualified Remote Signing and Sealing Services for Electronic Documents" comes into effect upon approval by the Board of Directors of Infonotary Ltd. and publication at: https://www.infonotary.com .

This document is valid until amended or its invalidity is published in the Document Registry and on the Provider's internet portal.

11.12.2. Termination

The Policy ceases to be effective upon termination of the Provider's activity.

11.12.3. Effect of Termination

In accordance with section 9.10.3 of the INFONOTARY document Certification practice statement for qualified certification services.

11.13. INDIVIDUAL NOTIFICATION AND COMMUNICATION BETWEEN PARTICIPANTS

In accordance with section 9.11 of the INFONOTARY document Certification practice statement for qualified certification services.

11.14. AMENDMENTS

This "Policy and Practice for Providing Qualified Remote Signing and Sealing Services for Electronic Documents" may be amended at any time. Each amendment is effective after approval by the Board of Directors of Infonotary Ltd. and is publicly accessible at: https://www.infonotary.com

Any person may submit proposals for changes (structural or substantive) and comments on identified errors to the Provider's contact emails and postal addresses specified in this document.

11.15. DISPUTE RESOLUTION AND JURISDICTION

In accordance with section 9.13 of the INFONOTARY document Certification practice statement for qualified certification services.

11.16. APPLICABLE LAW

In accordance with section 9.14 of the INFONOTARY document Certification practice statement for qualified certification services.

11.17. COMPLIANCE WITH APPLICABLE LAW

This "Policy and Practice for Providing Qualified Remote Signing and Sealing Services for Electronic Documents" is developed in accordance with Regulation (EU) No 910/2014 and national legislation.

11.18. OTHER PROVISIONS

This document contains no other provisions.