InfoNotary

POLICY AND PRACTICE FOR THE PROVISION OF A NATIONALLY QUALIFIED TRUST SERVICE FOR ELECTRONIC IDENTIFICATION

OF THE QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

Version 1.3

Effective from 15.09.2025

TABLE OF CONTENTS

1. INTRODUCTION

The main purpose of this document — POLICY AND PRACTICE FOR THE PROVISION OF A NATIONALLY QUALIFIED TRUST SERVICE FOR ELECTRONIC IDENTIFICATION by the Trust Service Provider INFONOTARY PLC (INFONOTARY/the Provider), is to describe and make publicly available:

- the conditions and procedures established and implemented by INFONOTARY in the provision of the electronic identification trust service (Electronic Identification Service / the Service / Identification Service);
- the applicability, security level, and limitations of the use of the Service;
- the specific operational rules and procedures followed by INFONOTARY in issuing and managing electronic identification means and in providing the Service;
- mechanisms for establishing the Provider's compliance — including its reliability and security — with the provisions and requirements of Regulation (EU) No 910/2014 and the relevant Bulgarian national legislation.

This document complements and shall be read in conjunction with the currently published versions of the following INFONOTARY documents: Certification Practice Statement for Qualified Trust Services, Policy for provision of qualified certificate for the qualified electronic signature, Policy and Practice for the Provision of a Nationally Qualified Remote Video Identification Service and Policy and Practice for providing a Service for Remote Signing and Sealing of Electronic Documents.

These documents contain the general terms and procedural requirements for user identification, issuance and management of qualified certificates, security requirements, and the generation and storage of key pairs (private and public) for such certificates, as well as their use in remote electronic document signing. Relevant references to sections of the above documents are provided where applicable.

The Policy and Practice Statement for the Provision of a Nationally Qualified Trust Service for Electronic Identification is a public document and may be updated when necessary. Any such changes are made publicly available to all interested parties at: https://www.infonotary.com.

This Policy and Practice is prepared in accordance with the provisions and requirements of the following European and national legal acts and standards:

- 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/ Regulation (EC) № 910/2014);
- 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;
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015

laying down minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014;

- Electronic Identification Act;
- Electronic Governance Act;
- Electronic Document and Electronic Trust Services Act;
- Measures Against Money Laundering Act, Article 55(2);
- Regulation for the Implementation of the Measures Against Money Laundering Act, (Article 42);
- 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 v2.1.1 General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures"
- ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons";
- ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons";
- ETSI TS 119 612 V2.2.1: Electronic Signatures and Infrastructures (ESI); Trusted Lists (т. 5.5.1.3 (g));
- Recommendation ITU-T X.509/ISO/IEC 9594-8: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks";
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework;
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP;
- RFC 3279: Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

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

1.1. MAIN PROVISIONS

1.1.1. Trust Service Provider and Electronic Identification 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 9001:2015 and its Information Security Management System, certified according to ISO/IEC 27001:2022.

1.2. Document Naming and Identification

The document — POLICY AND PRACTICE FOR THE PROVISION OF A NATIONALLY QUALIFIED TRUST SERVICE FOR ELECTRONIC IDENTIFICATION is titled **"InfoNotary eID service"** is identified by the following Object Identifier (OID): **1.3.6.1.4.1.22144.3.11**

Policy name	Identifier (OID)
InfoNotary eID service	1.3.6.1.4.1.22144.3.11

1.3. Participants in the Nationally Qualified Trust Service for Electronic Identification

1.3.1. Certification Authority

In accordance with section 1.3.1 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

1.3.2. Registration Authority

The Provider delivers the Electronic Identification Service to end users through a network of designated Registration Authorities.

The Provider's Registration Authorities perform the following activities:

- Receiving, approving, or rejecting applications from a natural person — the Applicant — either acting in a personal capacity, as an authorized representative of a legal entity or organization, or as a lawful representative of a legal entity or organization for the issuance of an electronic identification means;
- Creating a certified client profile of the Applicant within the Provider's systems, which serves as a means of electronic identification;
- Conducting identity verification of natural persons, and identity confirmation of legal entities and organizations, as well as of natural persons representing legal entities, using permissible means in connection with the provision of the electronic identification service. These verifications may also be conducted electronically (via a secure data exchange session) by sending requests and receiving information from a Trusted Information Source (Regix);
- Initiating issuance or revocation of cloud-based qualified certificates for qualified electronic signatures to confirm electronic identification (InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP) following successful verification and approval of the request, while notifying the Certification Authority;
- Generating asymmetric cryptographic key pairs on a remote device for secure electronic signature creation upon the request of the Certificate Holder;
- Concluding contracts for the provision of electronic identification services with

clients on behalf of and for the account of the Provider.

All or part of the registration activities may be performed by a Registration Authority of the Provider:

- at a physical office of the Registration Authority, in the personal presence of the Applicant for the trust service in a personal capacity, or as the lawful representative of a legal entity or organization;
- via the Provider's/Registration Authority's online information system or mobile application, which is accessible and used remotely by the Applicant for the electronic identification trust service, either in a personal capacity or as the lawful representative of a legal entity or organization. The Registration Authority may remotely verify the identity of the natural person through means of secure remote video identification, Qualified Electronic Signature Creation Devices (QESCD), and other legally valid means of secure remote identification.

The Provider may delegate rights and authorize third parties to act as Registration Authorities on behalf of and for the account of INFONOTARY PLC.

The Provider entrusts the activities of the Registration Authority based on a bilateral written agreement.

Authorized Registration Authorities conduct their activities in accordance with the InfoNotary Qualified CPS, the Provider's certification policies, and documented internal procedures and rules.

An up-to-date list of the Provider's authorized Registration Authorities is published and publicly accessible on the Provider's official website at https://www.infonotary.com.

Some functions of the Registration Authorities may be carried out by Local Registration Offices, which operate under the supervision of the Registration Authorities.

1.3.3. Electronic Identification Platform

The Electronic Identification Platform is a dedicated component (hardware and software) of INFONOTARY's trust infrastructure that performs the process of dynamic authentication (on-demand creation of electronic confirmation that the person/Holder controls the Electronic Identification Means and possesses the identification data), whereby the natural or legal person or organization uses the electronic identification means to confirm their identity to a relying party.

1.3.4. Holder of Electronic Identity

The "Holder" is a natural person of legal age, Bulgarian citizen, who has a verified user profile created in the Provider's systems and holds a cloud qualified certificate for confirmation of electronic identification (InfoNotary Qualified eID CP / InfoNotary Qualified Company eID CP) issued by the Provider, and is registered as such in the system.

1.3.5. Relying Parties (Electronic Service Providers)

A Relying Party is a legal entity or organization that provides electronic services and

relies on or requires electronic identification of the users of those services.

Relying Parties also include entities specified in Article 1, paragraphs 1 and 2 of the Electronic Governance Act, which require identification of persons and organizations to provide administrative services, in accordance with Article 5 of the Electronic Governance Act.

Relying Parties have access to the electronic identification service after signing an individual contract with the Provider, integration with INFONOTARY's Electronic Identification Platform, and definition of the data relating to natural persons, legal entities, and organizations that INFONOTARY will provide when using the respective electronic services.

Relying Parties should use a valid qualified website authentication certificate (SSL certificate), which will be used for authenticating the Relying Party when using the Electronic Identification Service.

1.3.6. Third Party

A legal entity, organization, administrative authority, or local government body, separate from the Provider, that trusts the trust services of INFONOTARY PLC and uses the electronic identification service in its own electronic processes.

Third Parties have access to the electronic identification service after signing an individual contract with the Provider, integration with INFONOTARY's Electronic Identification Platform, and definition of the data related to natural persons, legal entities, and organizations that INFONOTARY will provide when using the respective electronic services.

Third Parties should use a valid qualified website authentication certificate (SSL certificate), which will be used for authenticating the Third Party when using the Electronic Identification Service.

1.4. Use of Certificates

In accordance with section 1.4 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

1.4.1. Types of certificates and use

In accordance with section 1.4.1 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

1.4.2. Applicability, Use, and Accessibility of the Electronic Identification Service

The nationally qualified trust service for electronic identification (Electronic Identification Service / the Service) is provided through an electronic identification scheme managed by INFONOTARY, which meets the security and reliability requirements for remote verification and authentication of citizens' identities as defined in Regulation (EU) No 910/2014. The issued electronic identification means are certified at a "high" assurance level, according to Commission Implementing Regulation (EU) 2015/1502, which recognizes their legal validity and applicability in various electronic processes and services. The "high"

assurance level guarantees a high degree of reliability in proving persons' identities in electronic environments.

The electronic identification service can be used, after registration, by a natural person or a natural person representing a legal entity at any time and place via the InfoNotary SignZone mobile application.

In general, the electronic identification service is applicable in online processes requiring secure verification of the identity and authenticity of natural and legal persons or natural persons representing legal entities - e.g., usage of various electronic services, authentication before systems and applications, electronic authorization, and others.

The electronic identification means issued within the nationally qualified electronic identification trust service have a "high" assurance level and may be used by citizens and organizations according to the requirements of Article 5, paragraph 2, item 2 of the Electronic Governance Act, as means of identification when requesting electronic administrative services.

In accordance with Article 5, paragraph 3 of the Electronic Governance Act, electronic identification means issued by INFONOTARY are interoperable and integrated with the electronic authentication system established and maintained by the Ministry of Electronic Governance.

INFONOTARY's nationally qualified electronic identification trust service also meets the requirements of Article 13, paragraph 1, item (a) of Directive (EU) 2018/843, Article 55, paragraph 2 of the Law on Measures against Money Laundering, and Article 42 of the Rules for Implementation of the Law, enabling secure identity verification of persons during remote provision and use of various banking and financial services.

The service can be used by users, Holders of electronic identification means, who have concluded a contract with INFONOTARY, or by users for whom an organization has concluded a contract/agreement with INFONOTARY.

Relying parties/Third parties may use the electronic identification service after concluding a contract with INFONOTARY and must be authorized to process personal data of the holders of electronic identification means in accordance with applicable legislation.

Where practically feasible, the Provider ensures accessibility for persons with disabilities. Accessibility to services and products is provided without compromising or excluding compliance with security requirements, applicability, and conformity with Regulation (EU) No 910/2014, national legislation, and the Provider's internal policies and procedures.

1.4.3. Limitations on the Trust Service's Scope

The nationally qualified electronic identification trust service must not be used in a manner that violates the confidentiality and security of personal data.

The electronic identification means issued by the Provider have a limited scope of use — for electronic identification of the Holder and authentication in the virtual environment when accessing electronic services provided by Relying Parties / Electronic Service Providers.

The Provider is not responsible for damages arising from the use of the electronic identification service beyond the permitted use and within the limitations related to its intended purpose, especially when Relying Parties / Electronic Service Providers / Third Parties do not have the right and process users' data in violation of applicable legislation, which will result in the annulment of the guarantees provided by INFONOTARY to users and relying parties.

1.5. Management of the Trust Policy of the Electronic Identification Service Provider

The trust policy of the Provider is determined by the Board of Directors of INFONOTARY EAD.

All changes, edits, and additions to this Policy are approved by the Board of Directors of INFONOTARY EAD.

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

All comments, requests for information, and clarifications regarding this Policy may be addressed to: INFONOTARY PLC, 1000 Sofia, Bulgaria, 16, Ivan Vazov St., e-mail: legal@infonotary.com.

1.6. TERMS AND ABBREVIATIONS

Authentication,	An electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form
Authentic Source	Repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice. For the purposes of this document and the method of service provision, a trusted source is considered to be the official primary registers maintained by central government authorities (Ministries) and executive agencies, accessible through the Registry Information Exchange System (RegiX).

Dynamic Authentication pursuant to Implementing Regulation (EC) 2015/1502	An electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject/Holder is in control or in possession of the identification data and which changes with each authentication between the subject/Hoder and the system verifying the subject's/Holder's identity;
Electronic Identification Service Provider	Qualified Trust Service Provider that issues and manages an electronic identification means and ensures the process of dynamic authentication during electronic identification.
Electronic Identification, pursuant to Regulation (EU) No 2024/1183	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person
Electronic identity pursuant to Electronic Identification Act	A set of characteristics recorded in electronic form, based on which a person can be uniquely distinguished from other individuals in the virtual environment for the purpose of ensuring access to information systems or enabling the performance of electronic statements.
Electronic Identifier pursuant to Electronic Identification Act	A number, symbol, or characteristic assigned to a natural person for the purpose of their unique identification or for verifying their authenticity.
Electronic Identification Platform of the Provider	A distinct component (hardware and software) of INFONOTARY's certification infrastructure, which performs dynamic authentication and may maintain a register of authorizations.
Electronic Identification Means, pursuant to Regulation (EU) No 2024/1183	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service. For the purposes of this document and the manner of providing the Service, the means of electronic identification is the created certified client profile in the InfoNotary systems.
Electronic Identification Scheme, pursuant to Regulation (EU) No 2024/1183	A system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons
Electronic Identity Holder, pursuant to Electronic Identification Act	A natural person of legal age to whom an electronic identification means has been issued

Person identification data, pursuant to Regulation (EU) No 2024/1183	A set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.
Mobile Application InfoNotary SignZone	Specifically developed software by the Provider, intended for the secure delivery and use of the Provider's trust services, published in the respective mobile application stores for the Android, iOS, operating systems.
Provider of Electronic Service	An entity that provides electronic services and acts as a Relying Party in relation to the electronic identification service.
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body
Qualified Trust Service	A trust service that meets the applicable requirements laid down in Regulation (EU) № 2024/1183
Relying Party, pursuant to Regulation (EU) No 2024/1183	A natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service
Secure Electronic Identity Storage Device	Configured software or hardware used to store the electronic identification means and protect the private key from unauthorized access, copying, or tampering. SSCD/QSCD-certified devices may also be used in accordance with Regulation (EU) No 910/2014.
Trust Service, pursuant to Regulation (EU) № 2024/1183	An electronic service, usually provided for remuneration, consisting of one or more of the elements listed in Article 3, point 16 of Regulation (EU) 2024/1183.
User, pursuant to Regulation (EU) № 2024/1183	A natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with Regulation (EU) № 2024/1183
Regulation GDPR	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)

eIDAS Regulations	Means a pursuant to the following two regulations: 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/ Regulation (EC) № 910/2014); Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a framework for a European Digital Identity (eIDAS 2.0 Regulation);

ABBREVIATIONS

PIN	Personal Identification Number
eID	Electronic Identification
TSP	Trust service provider
eIDC	Electronic identity certificate
eIDM	Electronic identification means
eIDSSD	Electronic identity secure storage device
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
Cloud QES	Cloud qualified electronic signature

2. OBLIGATIONS FOR PUBLICATION AND MAINTENANCE OF REGISTERS

In accordance with section 2 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

When issuing the cloud-based qualified certificates InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP, the Provider follows the rules and conditions specified in section 3.1 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

3.2. Initial Identification and Identity Verification

Initial identification and verification of the identity of persons during the issuance of an electronic identification means (eIDM) and the cloud-based qualified certificates InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP is performed by the Applicant choosing one of the following methods:

1. Personal appearance of the Applicant at an INFONOTARY Registration Authority office;

2. Remote video identification via the INFONOTARY's Mobile Application.

3.2.1. Identity verification of Natural/Legal Person by personal appearance at an INFONOTARY's Registration Authority Office

In accordance with section 3.2 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

3.2.2. Identity verification of Natural/Legal person by Remote Video Identification

In accordance with section 4.2 of the document Policy and Practice for the Provision of a Nationally Qualified Remote Video Identification Service.

3.3. Identification and Authentication in a request for key replacement in a certificate

In accordance with section 4.3 of the Policy and Practice for the Provision of a Nationally Qualified Remote Video Identification Service.

3.4. Identification and Authentication in a request for termination of eIDM and certificate

The termination of the electronic identification means and the cloud-based qualified certificates InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP is performed by the Holder after successfully completing a remote video identification process or by personal appearance of the Holder at an INFONOTARY's registration office.

4. OPERATIONAL CONDITIONS

Operational activities in providing the electronic identification service include: providing access to download the InfoNotary SignZone, identification and verification of the Applicant's identity, creation of the electronic identification means and authentication when using the eIDM.

4.1. Downloading the Mobile Application - InfoNotary SignZone

The InfoNotary SignZone is published in the App Store and Google Play electronic stores, and depending on the operating system of the smart device used by the Holder of eIDM, they can download and install it.

4.2. Procedures for Requesting and Terminating an Electronic Identification Means

4.2.1. Procedure for Issuing an Electronic Identification Means

The procedure begins with the Applicant's registration in the mobile application, which includes a remote video identification process.

After successful verification and confirmation of the Applicant's identity, the Registering Authority creates a verified user profile, i.e., the electronic identification means, in the PROVIDER's systems and submits a request for issuing a cloud-qualified certificate for qualified electronic signature to confirm the identification — InfoNotary Qualified eID CP or InfoNotary Qualified Company eID CP to the Operational Certification Authorities InfoNotary Qualified Personal Sign CA or InfoNotary Qualified Personal Sign CA G3 and confirms that:

- the issuance request originates from the Holder;
- the information regarding the Holder is true and complete;
- the private key is technically suitable for use in authenticating the Holder's electronic identity during the authentication process;
- the private key is held by the Holder;
- the Holder has means under their control for personal remote access to the private key in the Provider's HSM via the InfoNotary SignZone Mobile Application.

The action of the Operational Certification Authority is in accordance with section 4.3.1 of the Certification Practice Statement for Qualified Certification Services.

In the Mobile Application, the User/Client is notified that their identification was successful, the registration is complete, and they have an electronic identification means and issued qualified certificates for cloud qualified electronic signature.

If the process of confirming the issuance request of the eIDM fails, the Registering Authority rejects the issuance request and notifies the User/Client, stating the reason for

rejection. After rectifying the reasons that caused the unsuccessful identification, the User/Client may restart the process via InfoNotary SignZone.

The Registering Authority records and stores information, data, and digital copies of documents provided by the Holder during the remote identification process.

The Holder has the ongoing obligation to ensure the accuracy of the provided information and to inform the Provider of any changes occurring after the issuance of the eIDM.

The Provider issues the electronic identification means and cloud-qualified certificates immediately after the User/Client identity has been confirmed by the Registering Authority.

4.3. Acceptance and Publication of the Certificate

4.3.1. Acceptance of the Certificate

In accordance with section 4.4.3 of the INFONOTARY document Certification practice statement for qualified certification services".

4.3.2. Publication of the Certificate

In accordance with section 4.4.2 of the INFONOTARY document Certification practice statement for qualified certification services.

4.4. Data Confidentiality

In accordance with section 4.5 of the INFONOTARY document Certification practice statement for qualified certification services.

4.5. Renewal of Electronic Identification Means and Certificate

The electronic identification means and cloud-qualified certificates are not subject to renewal. The Provider issues a new eIDM and cloud certificate upon the User's/Client's request, following the initial procedure of identification and identity verification.

4.6. Key Replacement in Certificate and Certificate Modification

In accordance with sections 4.7 and 4.8 of the INFONOTARY document Certification practice statement for qualified certification services.

4.7. Termination of Electronic Identification Means and - Qualified Certificate for Cloud Qualified Electronic Signature InfoNotary Qualified eID CP/ InfoNotary Qualified Company eID CP

4.7.1. Procedure for Termination of Electronic Identification Means

The electronic identification means is terminated:

- at the request of the Holder by deleting/deactivating the user profile or

terminating the concluded electronic identification service contract via the Mobile Application. For this purpose, the Holder must undergo a remote video identification process. In this way, the Holder confirms the termination request of the eIDM before the Registering Authority. By deactivating the eIDM, the Holder also requests the termination of any existing valid qualified certificates for cloud-qualified electronic signature;

- upon expiration of the validity period of the issued qualified certificates for cloud-qualified electronic signature;
- upon the death or legal incapacitation of the Holder;
- upon termination of the legal entity when the eIDM was issued to a legal entity;
- upon termination of the Holder's representative authority concerning the legal entity when the eIDM was issued to that legal entity;
- upon establishing that the eIDM was issued based on false data;
- upon termination of the legal entity of the Provider of qualified trust services.

After termination of the eIDM and cloud certificates, the Provider notifies the Holder by email, in an online information system, or via the Provider's Mobile Application.

Electronic identification means and cloud certificates terminated by the Provider are not subject to renewal.

After termination of the qualified certificates for cloud-qualified electronic signature, the Provider includes them in the Certificates Revocation List and updates the publicly accessible electronic certificate register.

Deletion of the Mobile Application installed by the Holder on their mobile device does not mean deletion/deactivation of their electronic identification means.

4.7.2. Period within which the Certification Authority must process the termination request

In accordance with section 4.9.4 of the INFONOTARY document Certification practice statement for qualified certification services.

4.7.3. Certificate Revocation List

In accordance with sections 4.9.6, 4.9.7, 4.9.8 and 4.9.9 of the INFONOTARY document Certification practice statement for qualified certification services.

4.8. TERMINATION OF THE ELECTRONIC IDENTIFICATION SERVICE AGREEMENT

The agreement for the provision of qualified trust services and electronic identification services via the Provider's mobile application and/or online information system with the Holder is terminated if the eIDM is terminated or the issued cloud-qualified certificates have expired, as well as on other grounds stipulated in the agreement.

5. NATIONALLY QUALIFIED TRUST SERVICE FOR ELECTRONIC IDENTIFICATION

5.1. GENERAL CHARACTERISTICS AND DESCRIPTION

INFONOTARY, as a provider of a qualified at national level trust service for electronic identification (Electronic Identification Service/the Service), manages an electronic identification scheme that is part of the Provider's PKI infrastructure, built and audited in accordance with the requirements of eIADS Regulations, which is used to provide qualified trust services.

The electronic identification service is a combination of the following services, which can be provided together or separately:

- Issuance of an electronic identification means; and
- Dynamic authentication.

The electronic identification service is provided via INFONOTARY's Electronic Identification Platform the Mobile Application - InfoNotary SignZone or a mobile application integrating INFONOTARY's Software Development Kit (SDK), and includes:

- the User's/Client's registration process;
- creation of a verified user profile in the Provider's systems, which serves as an electronic identification means (eIDM) for a natural person, legal entity, or organization;
- issuance of cloud-qualified certificates InfoNotary Qualified eID CP/InfoNotary Qualified Company eID CP; and
- an online dynamic authentication process upon receiving an electronic identification request from a relying party/electronic service provider integrated with the Platform.

The service provision process is initiated by a natural person (User/Client) via the InfoNotary SignZone, through registration and submission of a request for issuance of an electronic identification means before the Provider's Registering Authority. The User/Client may be any natural person who is a Bulgarian citizen.

The Registration Authority initiates the procedure for initial identification and verification of the identities of natural persons, natural persons acting as legal representatives of legal entities/organizations, and the identities of legal entities, in compliance with the rules and procedures in this document, as well as other internal documents of the Provider.

INFONOTARY provides two methods for initial identification and identity verification of individuals, at the User's/Client's choice: **a)** in-person appearance of the User/Client at an INFONOTARY registration office; and **b)** remote video identification via the Provider's Mobile Application - InfoNotary SignZone.

The Registration Authority performs the remote video identification process in accordance with the Policy and Practice for the Provision of a Nationally Qualified Remote Video Identification Service of INFONOTARY.

Upon a positive result of the verification and confirmation of the User's/Client's identity, a verified user/client profile is created and a qualified certificate for cloud qualified electronic signature confirming the identification — InfoNotary Qualified eID CP or InfoNotary Qualified Company eID CP — is issued.

The Provider's registers maintain correspondence between the electronic identifier and the data about the natural person, which is collected and verified during the initial identification and identity confirmation process. Based on the electronic identifier, a unique distinction of one individual from others in the virtual environment can be made during the authentication process (described in section 5.2.5). This process is activated/performed by the Holder each time the electronic identifier/electronic identification means is presented to a Relying Party / Electronic service provider. The Holder may use the eIDM an unlimited number of times within its validity period.

When the Holder requests the use of an electronic or informational service, the information system of the Relying Party recognizes the Provider and sends, via API interface or SDK module, the identifier along with a request for providing specific identification data of the User. INFONOTARY performs a check in its registers to verify the correspondence between the electronic identifier and the Holder's data (e.g., full name, personal identification number, identity document number, gender, age, etc.). Then, the Provider contacts an Authentic source (RegiX) to verify/retrieve the current and valid data of the respective natural person at the time of the Relying Party's request. INFONOTARY displays a message in the Mobile Application under the control of the Holder, requesting the Holder's consent for identification. The message contains information about the Relying Party, the electronic service, and the current personal and other data requested by the electronic service. The Holder can either confirm or deny the provision of the data.

The Holder gives consent for the data provision by entering their secret code (PIN) created for: accessing the Application, expressing consent during electronic identification, and signing electronic documents, and signs it with their issued qualified certificate InfoNotary Qualified eID CP/InfoNotary Qualified Company eID CP. The signed consent contains the current data obtained from the Authentic source, as well as information about the intended recipient(s) of the data.

In this way, INFONOTARY guarantees that the information provided to the Relying Party during the dynamic authentication process has not been altered and is identical to the information received from the Authentic source. After confirmed consent, the Provider returns the verified and current data about the individual to the Relying Party in one of the following ways — as an electronic document in PDF format, signed by the Holder, or in a format suitable for machine processing — JSON, etc.

INFONOTARY provides the data about the individual to the Relying Party in an automated manner, in machine-readable or other format, according to the agreement between the parties.

The data that the Relying Party may request/receive through the Electronic Identification Service are as follows:

- For a natural person:

- First name, middle name, and family name (written in Bulgarian and Latin script);
- Date and place of birth;
- Nationality;
- Gender;
- Permanent address, city, country, postal code;
- National identification number;
- Identity document number: identity card, passport;
- Issuer, issue date, and validity of the identity document as of the request date;
- Validated mobile phone number;
- Validated email address.

➢ For a legal entity:

- Name of the legal entity;
- Legal form;
- Unique Identification Code (UIC/BULSTAT number);
- Names of official representatives;
- Address, city, country, postal code;
- Activity status.

INFONOTARY may supplement the set of data for natural persons, legal entities, and organizations with the consent of the Holders and provided access to additional primary registers and trusted data sources.

5.2. COMPONENTS OF THE ELECTRONIC IDENTIFICATION SERVICE

5.2.1. Electronic Identification Means (Certified User Profile)

After successful verification and confirmation of the User's/Client's identity, the Registration Authority creates a verified user profile in the Provider's systems, which serves as the electronic identification means in accordance with Article 3, paragraph 2 of Regulation (EU) 910/2014 (amendment with Regulation (EU) 2024/1183).

Together with the creation of the electronic identification means (eIDM), a qualified certificate for cloud qualified electronic signature (InfoNotary Qualified eID CP/InfoNotary Qualified Company eID CP), is issued in which the User/Client is registered as the Holder, and for which a key pair (public and private) is generated. The private key is protected for exclusive use by the Holder through a secret code (PIN) created by the Holder to access the application and to sign electronic documents with the cloud qualified electronic signature.

The Electronic Identification Means contains one or more unique identifiers of the natural person (Holder of the Means) and other personal identification data necessary for the identification and use of the requested certification services, including information about the issued cloud qualified electronic signature (Cloud QES).

The Electronic Identification Means is considered active when the Holder has valid Cloud QES issued.

The eIDM is considered inactive when the Holder's issued Cloud QES have expired or when the Holder has voluntarily terminated the eIDM. In such cases, the Holder's access to the eIDM is revoked, and all data and documents related to the Holder are deleted from the InfoNotary systems.

The eIDM is protected against duplication and forgery by using cryptographic keys and algorithms, as well as comprehensive security measures (firewalls, backup systems, and other software and hardware solutions) employed to secure the Provider's infrastructure.

Use of the eIDM is activated by the Holder through the use of the private key, which is solely under their control and protected by a PIN known only to the Holder. Therefore, it is assumed that the eIDM is used exclusively under the control and possession of the Holder to whom it belongs.

5.2.2. Electronic Identifier

The electronic identifier of the Holder may be a unique number automatically generated after confirmation by the Registration Authority during the creation of the user profile and is unique within the Provider's register (User Identification Number – UIN), or it may be the unique personal identification number of a natural person (EGN), or the unique identifier of a legal entity or organization (UIC/BULSTAT number). The Holder can choose which electronic identifier to present to the Relying Parties.

5.2.3. Qualified Certificate for Qualified Electronic Signature to Confirm Electronic Identification InfoNotary Qualified eID CP/ InfoNotary Qualified Company eID CP

The Cloud QES to confirm electronic identification (InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP), are issued to a natural person, the Holder of the electronic identification means, either in a personal capacity or as a lawful/authorized representative of a legal entity or organization. The Holder uses the issued certificate in the process of authentication by remotely signing a specific set of verified and up-to-date data before they are sent by the Provider to the Relying Party/Electronic service provider.

Each of the Cloud QES is associated with a pair of cryptographic keys, which are generated and stored exclusively in a hardware security module (HSM) with a security level of CC EAL 4+ or higher. The HSM is managed by the Provider on behalf of the Holder under appropriate mechanisms and procedures implemented in accordance with Regulation (EU) 910/2014 (amendment with Regulation (EU) 2024/1183), ensuring that the Holder has sole control over the use of the data to activate the private key.

The Cloud QES (InfoNotary Qualified eID CP and InfoNotary Qualified Company eID CP) is issued with a validity period of 3 years.

The data for remote activation of the private key (the secret code (PIN) created by the Holder for access to the Mobile Application, for giving consent during electronic identification, and for signing electronic documents) are known and accessible solely to the Holder and are under the exclusive control of the electronic identity Holder.

5.2.4. Mobile Application

The mobile application InfoNotary SignZone is specially developed by the Provider software designed for reliable provision and use of trust services. The mobile application is also developed as an SDK version (InfoNotary Mobile SDK), which allows integration of the application's functionalities into third-party mobile applications. The InfoNotary SignZone application is available for download and use on mobile smart devices with Android and iOS operating systems.

The electronic identification service is part of the Provider's certification services delivered through InfoNotary SignZone. The mobile application provides a secure and controlled environment that guarantees the authenticity, integrity, and confidentiality of the authentication process.

The mobile application requires the User/Client to create a secret code (PIN) for access/login to the Application, for giving consent during electronic identification, and for signing electronic documents with a cloud qualified electronic signature.

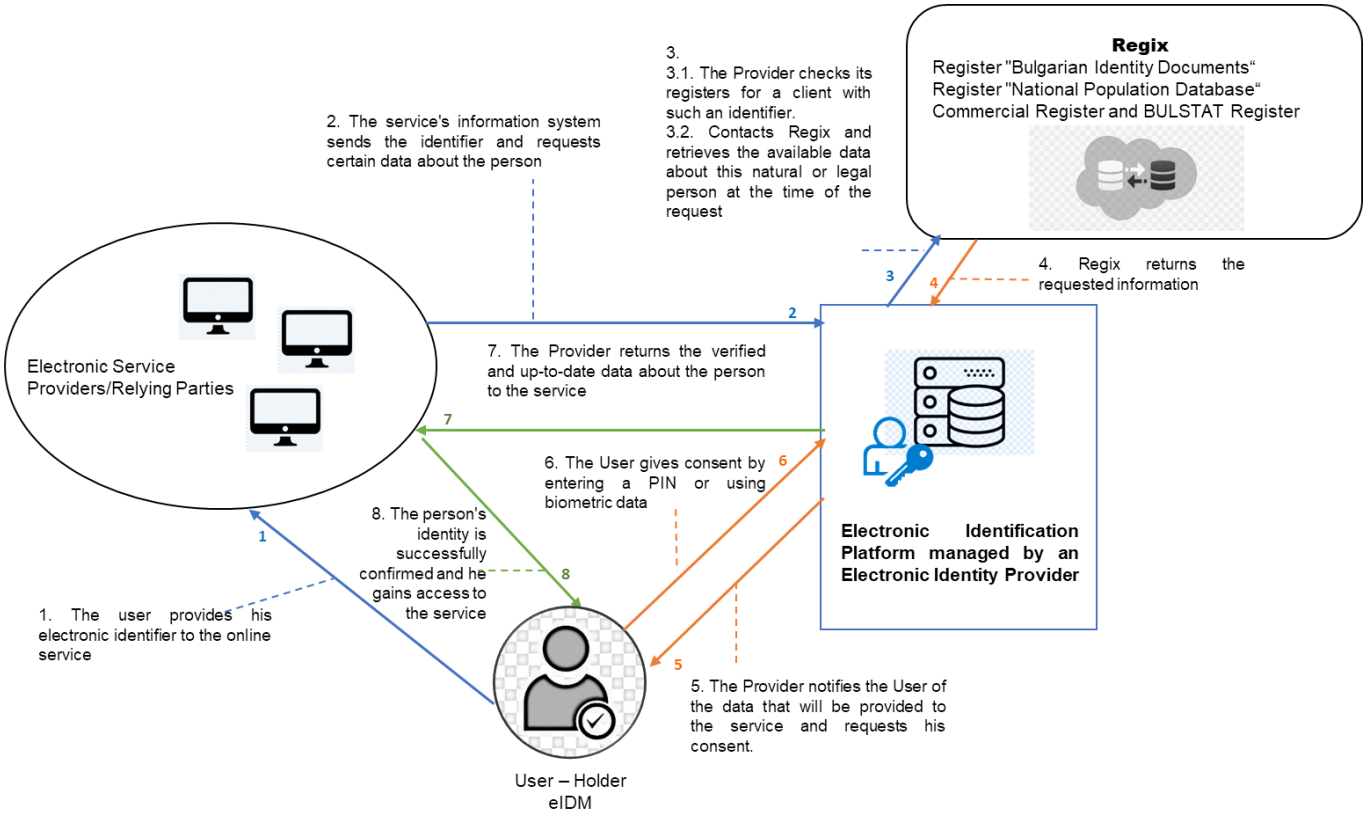
Through the mobile application, User/Client can register for the issuance of an electronic identification means, and the Holders of electronic identification means can confirm the provision of a specific set of data by the Provider, which allows establishing their identity during the authentication process.

5.2.5. Dynamic Authentication Process/Service

The dynamic authentication process is executed by the InfoNotary Platform online (in real-time) each time the electronic identification means is used by a natural or legal person. Valid data about the respective person, current at the time of the request, are returned/provided to the information system through which the electronic service is offered, after obtaining proper consent from the Holder of the electronic identification means (eIDM). This consent confirms that the Holder wishes the electronic identification service provider to deliver a specific set of data that allows establishing the identity of a natural or legal person, or a natural person representing a legal entity.

The consent or refusal to provide data from the electronic identification service provider to a third party is given by the Holder, based on a conscious choice of exactly to whom the data will be provided and what data will be disclosed (e.g., full name, unique identifier, gender, age, etc.).

A diagram of the authentication process is shown below:



Scheme 1

5.3. USE OF THE ELECTRONIC IDENTIFICATION MEANS (eIDM)

The Holder may use the eIDM, during its validity period, an unlimited number of times by presenting their electronic identifier to a Relying Party / Electronic Service Provider.

The Holder receives a message in the Mobile Application requesting their consent for identification, i.e., for providing a specific set of data to the Relying Party / Electronic Service Provider. The Holder can confirm or refuse to provide the data.

The Holder gives consent by entering the secret code (PIN) they created.

If the Holder refuses to provide data, entering the PIN is not required.

The Holder must not share the created PIN with third parties. From the moment the secret code is created, the Holder is personally and solely responsible for the secrecy and protection of their PIN, as well as for all actions performed by them or by third parties using it. Any use of the PIN is considered an action of the Holder. The Provider is not responsible for the use of the PIN by the Holder or for any unauthorized use of the PIN by the Holder.

If the Holder enters an incorrect PIN 3 (three) consecutive times when accessing the Application, confirming consent for identification, or signing documents, access or the ability to log in, confirm, and sign will be restricted for a certain period of time. After this period expires, the restriction is lifted and the Holder may try again.

The Holder may change the PIN they created during registration by using the corresponding functionality in the "Settings" of the Application.

If the Holder forgets the PIN or suspects it has been compromised, they may create a new PIN by going through the remote video identification process again. In this case, the issued certificates managed with the old PIN will be revoked and new ones issued.

The PIN chosen by the Holder is used to manage their eIDM and cloud certificates across all mobile devices where the Holder has installed and activated the InfoNotary mobile application. When the PIN is changed on one device, the new PIN is used on all other devices as well.

The Holder may use the eIDM, during its validity period, an unlimited number of times by presenting their electronic identifier to a Relying Party/Electronic Service Provider.

Relying Parties/Electronic Service Providers and Third Parties, upon receiving the electronic identifier from the Holder of the eIDM, access the InfoNotary Electronic Identification Platform via an integrated channel to request dynamic authentication of the Holder of the eIDM, specifying the particular data of the Holder to be provided. After receiving proper consent from the Holder of the eIDM, the Platform sends the data to the Relying Parties and Third Parties.

6. CONTROL OF EQUIPMENT, PROCEDURES AND MANAGEMENT

The electronic identification scheme established and managed by INFONOTARY is part of the Provider's PKI infrastructure, which is built and audited in accordance with the requirements of the Regulation and is used to provide qualified trust services. In this regard, the rules and procedures described in the INFONOTARY document "Practice for Providing Qualified Trust Services" apply for the management and operational control of the equipment, its security, and its activities. This document supplements, where applicable, some of the specified rules and procedures, considering the functionality of the service.

6.1. PHYSICAL CONTROL

In accordance with item 5.1 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

6.1.1. Location and construction of premises

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

6.1.2. Physical access

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

6.1.3. Power supply and climatic conditions

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

6.1.4. Flooding

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

6.1.5. Fire alarm and protection

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

6.1.6. Data storage

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

6.1.7. Decommissioning of technical components

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

6.1.8. Duplication of components

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

6.2. PROCEDURAL CONTROL

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

6.2.1. Positions and functions

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

6.2.2. Number of personnel per task

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

6.2.3. Identification and authentication for each position

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

6.2.4. 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.

6.3. PERSONNEL CONTROL, QUALIFICATION, AND TRAINING

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

Employees of INFONOTARY who perform activities related to providing the eID Service and the maintenance and support of the Provider's information and technological systems

possess the necessary professional training and experience and comply with the approved internal operational requirements and procedures.

6.3.1. Requirements for independent suppliers

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

6.3.2. Documentation provided to employees

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

6.4. 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.

6.4.1. Frequency of record creation

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

6.4.2. Retention period of records

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

6.4.3. Protection of records

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

6.4.4. Procedure for creating backups of records

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

6.5. ARCHIVING

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

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

6.5.1. Types of archives

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

6.5.2. Retention period

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

6.5.3. Archive protection

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

6.5.4. Archive recovery procedures

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

6.5.5. 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".

6.5.6. Archive storage

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

6.5.7. 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".

6.6. CERTIFICATE KEY CHANGE

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

6.7. 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.

6.8. PROCEDURES FOR TERMINATION OF PROVIDER'S ACTIVITIES

6.8.1. Termination of activities

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

6.8.2. 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.

6.8.3. Revocation of the Provider's qualified status

In accordance with section 5.8.3 of the INFONOTARY document Certification practice statement for qualified certification services.

7. TECHNICAL AND COMPUTER SECURITY CONTROL

7.1. GENERATION AND INSTALLATION OF KEY PAIRS

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

7.1.1. Key pair generation

In accordance with section 6.1.1 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1.2. Delivery of the private key

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

7.1.3. Delivery of the public key

In accordance with section 6.1.3 of the INFONOTARY document Certification practice statement for qualified certification services".

7.1.4. Delivery of the Certification Authority Public Key to Relying Parties

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

7.1.5. Key length

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

7.2. PROTECTION OF THE PRIVATE KEY AND TECHNICAL CONTROL OF THE CRYPTOGRAPHIC

7.2.1. Cryptographic module standards

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

7.2.2. 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.

7.2.3. Storage of private keys

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

7.2.4. Archiving of private keys

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

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

In accordance with section 6.2.5 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2.6. Activation and Deactivation of Private Keys

In accordance with section 6.2.5 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2.7. Destruction of Private Keys

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

7.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

7.3.1. Archiving of the Public Key

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

7.3.2. 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".

7.4. ACTIVATION DATA

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

7.5. COMPUTER SECURITY CONTROL

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

7.6. TECHNICAL CONTROL AND LIFECYCLE

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

7.7. NETWORK SECURITY CONTROL

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

8. PROFILES

8.1. PROFILES OF QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURES OF NATURAL PERSONS FOR ELECTRONIC IDENTIFICATION CONFIRMATION

8.1.1. Profile of a qualified certificate for a qualified electronic signature of a natural person for electronic identification confirmation InfoNotary Qualified eID CP

InfoNotary Qualified eID 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 + 1 hour, 1, 2 or 3 years
Signature Algorithm		SHA256/RSA
Issuer:		
Attribute		Value
Domain Component	DC	qualified-natural-ca, qualified-natural-ca-g3
Common Name	CN	InfoNotary Qualified Personal Sign CA, InfoNotary Qualified Personal Sign CA G3
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Domain Component	DC	qualified-natural-ca, qualified-natural-ca-g3
Common Name	CN	Full name

Country Name	C	
Serial Number	2.5.4.5	IN:BG-XXXXXXXXXX (CIN – customer identification number)

Additional attributes of x509 extensions (x509v3 extensions):	
Attribute	Value
Basic Constraints (Critical)	End entity
Key Usage (Critical)	Digital Signature, Non-Repudiation
Public Key	RSA 2048 bits, RSA 3072 bits, RSA 4096 bits
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/qualified-natural-ca.crt URL=https://repository.infonotary.com/qualified-natural-ca-g3.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/qualified-natural-ca.crl URL=http://crl.infonotary.com/crl/qualified-natural-ca-g3.crl

Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=InfoNotary Qualified eID Certificate [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [3] Certificate Policy: Policy Identifier=0.4.0.1456.1.1
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcRetentionPeriod (oid=0.4.0.1862.1.3) id-etsi- qcs-QcLimitValue (oid=0.4.0.1862.1.2) Value: 25000 EUR id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	

8.1.2. Profile of a qualified certificate for a qualified electronic signature of a natural person with delegated powers for for electronic identification confirmation InfoNotary Qualified Company eID CP

InfoNotary Qualified Company eID 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 + 1 hour, 1, 2 or 3 years
Signature Algorithm		SHA256/RSA
Issuer:		
Attribute		Value
Domain Component	DC	qualified-natural-ca, qualified-natural-ca-g3
Common Name	CN	InfoNotary Qualified Personal Sign CA, InfoNotary Qualified Personal Sign CA G3
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		Value
Domain Component	DC	qualified-natural-ca, qualified-natural-ca-g3
Common Name	CN	Full name
Country Name	C	

Serial Number	2.5.4.5	IN:BG-XXXXXXXXXX (CIN – customer identification number)
Organization	O	
Organization Identifier	2.5.4.97	NTRYY-XXXXXXXXXX (National Identification Code) YY – Country code
Additional attributes of x509 extensions (x509v3 extensions):		
Attribute	Value	
Basic Constraints (Critical)	End entity	
Key Usage (Critical)	Digital Signature, Non-Repudiation	
Public Key	RSA 2048 bits, RSA 3072 bits, RSA 4096 bits	
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/qualified-natural-ca.crt URL=https://repository.infonotary.com/qualified-natural-ca-g3.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/qualified-natural-ca.crl URL=http://crl.infonotary.com/crl/qualified-natural-ca-g3.crl	

Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=InfoNotary Qualified Company eID Certificate [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [3] Certificate Policy: Policy Identifier=0.4.0.1456.1.1
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcRetentionPeriod (oid=0.4.0.1862.1.3) id-etsi- qcs-QcLimitValue (oid=0.4.0.1862.1.2) Value: 25000 EUR id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	

9. MONITORING AND CONTROL OF ACTIVITIES

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

9.1. REGULAR OR EXTRAORDINARY AUDIT

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

9.2. QUALIFICATION OF AUDITORS

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

9.3. 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.

9.4. SCOPE OF THE AUDIT

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

9.5. TAKING ACTIONS TO CORRECT DEFICIENCIES

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

10. OTHER BUSINESS AND LEGAL TERMS

10.1. PRICES AND FEES

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

10.1.1. 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.

10.1.2. Invoicing

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

10.1.3. Policy for Certificate Return and Refund

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

10.2. FINANCIAL RESPONSIBILITIES

10.2.1. Financial Responsibilities

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

INFONOTARY is responsible for the provided eID service towards all third parties relying on the performed identification, as well as towards any natural or legal person for damages caused due to failures in verifying the identity of the individual.

10.2.2. Insurance of Activity

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

10.2.3. Insurance Coverage for End Users

In accordance with section 9.2.2 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 the Holder/Relying Party/Third Parties in using the eID Service arising from the conditions of this document, the Practice for Providing Qualified Trust Services, the Provider's Policy and Practice for Remote Video Identification, the General Terms of Use of the InfoNotary SignZone application, and the individual contract concluded;
- loss of a mobile device or compromise of the secret code (PIN) created for accessing the application by the Holder, due to failure to exercise due care in its protection or use;
- malicious actions by third parties (hacker attacks, theft of the mobile device, access to the identification method, etc.);
- unlawful actions by the Holder/Relying Parties/Third Parties;
- untimely request by the Holder to the eID Service to suspend/terminate access to the mobile application, as well as termination of issued eID credentials and certificates;
- force majeure, accidents, and other events beyond the Provider's control.

10.3. CONFIDENTIALITY OF INFORMATION

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

10.3.1. 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 any information contained in or related to any data about the Applicant/User/Client of the Provider's Electronic Identification Service, except for the information included in the result of the electronic identification process;

10.3.2. 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.

10.3.3. Obligation to Protect Confidential Information

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

10.4. PERSONAL DATA PRIVACY

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

10.5. INTELLECTUAL PROPERTY RIGHTS

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

10.6. OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES

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

10.6.1. Provider's Obligations, Responsibilities, and Warranties

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

When providing the eID Service, the Provider guarantees the correct identification of the persons at the time of providing the service

10.6.2. 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.

10.6.3. Obligations and Responsibilities of the Holders of the eIDM

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

Additionally, the Holder of eIDM, when using the Electronic Identification Service, has the following obligations and responsibilities:

- To comply with the terms of this document, the Practice for Providing Qualified Certification Services, the Policy and Practice for Remote Video Identification, the General Terms of Use of the Mobile Application, and the Privacy and Personal Data Protection Policy;
- To provide true, accurate, and complete information required by the Provider in accordance with regulatory requirements and applicable Policies and Practices;
- Not to make false statements or submit counterfeit documents to the Registration Authority related to the provision of the service;
- To strictly follow the security requirements established by the Provider;
- To keep the created secret code (PIN) safe from disclosure or unauthorized use;

- To promptly request from the Provider the suspension or termination of access to the mobile application or the termination of the QEI and certificate when the Holder becomes aware that the created PIN has been compromised, misused, or there is a risk of unauthorized use.

The Holder of eIDM is liable to InfoNotary in all cases of failure to fulfill the above obligations arising from this document, the Certification practice statement for qualified certification services, the Policy and Practice for the Provision of Remote Video Identification Service, and the General Terms of Use of the InfoNotary SignZone application, with the Provider holding the User/Holder responsible for any damages.

10.6.4. Obligations and Responsibilities of 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.

10.7. DISCLAIMER OF LIABILITY

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 the Users of the Electronic Identification Service to comply with the obligations arising from the terms of this document, the Practice for Providing Qualified Certification Services, the Provider's Policy and Practice for Remote Video Identification, and the General Terms of Use of the InfoNotary SignZone application;
- Loss of a mobile device or compromise of the created secret code (PIN) for accessing the application by the user, due to failure to exercise due care in safeguarding or using it;
- Malicious actions by third parties (hacking attacks, theft of mobile devices, unauthorized access to identification methods, etc.);
- Illegal actions by Users and Relying Parties;
- Force majeure, accidents, and other events beyond the control of the Provider

The Provider is not responsible for damages incurred by the Relying Party/Third Party resulting from the failure to fulfill obligations and the lack of due care defined in the concluded contract.

10.8. LIMITATION OF LIABILITY

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

10.9. COMPENSATIONS TO THE PROVIDER

In all cases of failure to fulfill obligations by the Users of the Electronic

Identification Service and Third Parties arising from the conditions of this document, the Provider's Practice for Providing Qualified Certification Services, and the General Terms of Use of Qualified Certification Services via the mobile application, the Provider shall hold the Users of the Service and Third Parties liable for damages.

10.10. TERM AND TERMINATION

10.10.1. Terms

This "Policy and Practice for Provision a Nationally Qualified Trust Service for Electronic Identification" enters into force from the moment of its approval by the Board of Directors of Infonotary PLC and its publication at: http://www.infonotary.com.

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

10.10.2. Termination

This "Policy and Practice for Provision a Nationally Qualified Trust Service for Electronic Identification" ceases to be effective upon termination of the Provider's activity.

10.10.3. Effect of termination

After termination of its effect for users, the provisions regarding the Provider's obligations to maintain an archive of documents and information, in the scope and period described in this document, remain in force.

10.11. INDIVIDUAL NOTIFICATION AND COMMUNICATION BETWEEN PARTICIPANTS

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

10.12. AMENDMENTS

This "Policy and Practice for Provision a Nationally Qualified Trust Service for Electronic Identification" may be amended at any time, with each amendment coming into effect after approval by the Board of Directors of Infonotary EAD and being publicly accessible to all interested parties at https://www.infonotary.com

Any person may submit proposals for changes (structural and substantive) and notes on detected errors to the contact email and postal addresses indicated in this document.

10.13. DISPUTE RESOLUTION AND JURISDICTION

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

10.14. APPLICABLE LAW

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

10.15. COMPLIANCE WITH APPLICABLE LAW

This "Policy and Practice for Provision a Nationally Qualified Trust Service for Electronic Identification" is developed in accordance with the requirements of Regulation (EU) 910/2014 (amendment with Regulation 2024/1183) and national legislation.

10.16. OTHER PROVISIONS

This document contains no other provisions.