# Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service "Management of remote electronic signature/seal creation devices"

**Version 1.0**

**Effective date: March 15, 2026**



**Asseco Data Systems S.A.**
Jana z Kolna Street 11,
80-864 Gdańsk, Poland
www.assecods.pl
**Certum**

Bajeczna Street 13
71-838 Szczecin, Poland
www.certum.pl
www.certum.eu

## Trademark and Copyright notice

# Content

## 1. Introduction

Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service "Management of remote electronic signature/seal creation devices", hereinafter referred to as **the RQSCD Policy**, is a document that bases and supplements the "Certification Policy and Certification Practice Statement of Certum Qualified Services", hereinafter referred to as **the Main Policy**, which defines the general rules applied by Certum during the provision of qualified trust services. This document also acts as a Certification Policy for each type of qualified certificates and for the service of issuing **qualified certificates in the signing process**, including registration of **service recipients** and certification of public keys.

These services are provided in accordance with:

- the Integrated Management System, implemented by Asseco Data Systems S.A., which includes the requirements of the PN-EN ISO 9001:2009 and PN-ISO/IEC 27001:2014,
- the *Regulation of the Ministry of Digitalisation of 5th October 2016 according the National Trust Infrastructure,*
- *the Act on Trust Services and Electronic Identification (Dz.U. 2019 r. poz. 162),*
- the services mentioned above are provided in accordance with the requirements of the *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* and with *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation as regards establishing the European Digital Identity Framework*, hereinafter referred to as the *eIDAS Regulation*,
- the services listed above are provided in accordance with the requirements of Commission Implementing Regulation (EU) 2025/1567 of July 29, 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council with regard to the management of qualified remote electronic signature devices and qualified remote electronic seal devices as qualified trust services.

The Main Policy defines parties, their obligations and responsibilities, types of certificates, authentication procedures and applicability range. The knowledge of the nature, purpose and role of The Main Policy is particularly important for a **subscriber** and a **relying party**[1].

The structure and substantive content of the RQSCD Policy comply with the recommendations of RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. It also meets the requirements of the *ETSI TS 119 431-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.*

This document was created assuming that the reader is generally familiar with the notions concerning certificates, certificate evidences, electronic signatures and a Public Key Infrastructure (**PKI**).

*Applicable notions, terms and their meaning are defined in the **Glossary** at the end of this document.*

[1] A service recipient who is acting on the basis of trust in the certificate and digital signature.

### 1.1. Overview

The RQSCD Policy describes the scope of activities that must be undertaken by Certum, registration authorities, subscribers and relying parties in order to meet the highest legal and standardization standards.

### 1.2. Document Name and its Identification

The present document is given a proper name of **Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service "Management of remote electronic signature/seal creation devices"** and is available in an electronic version at: www.certum.eu.

The following registered object identifier relates to the above-mentioned document (OID: 1.2.616.1.113527.2.4.1.0.6.1.0):

> **id-cck-kpc-v1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-kpc(pc)(6) version(1) 0}**

in which the two last numeric values correspond to the current version and subversion of this document.

### 1.3. Statement of Conformity for Server Signature Service Policies

Asseco Data Systems SA, as a provider of the qualified service "Management of remote electronic signature/seal creation devices," declares its compliance with the EUSPv2 policy:

**itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)**

### 1.4. RQSCD Policy Parties

The Main Policy regulates the most important relations between the entities belonging to Certum, its advisory teams (including auditors) and customers (users of supplied services). The regulations particularly apply to:

- services for of remote electronic signature or seal creation devices,
- subscribers,
- relying parties.

#### 1.4.1. Subscribers

The scope related to this chapter was addressed in the Main Policy.

#### 1.4.2. Relying Parties

The scope related to this chapter was addressed in the Main Policy.

#### 1.4.3. Other Parties

The scope related to this chapter was addressed in the Main Policy.

### 1.5. Certificate Policy and Certification Practice Statement Administration

RQSCD Policy is administered on the terms described in the Main Policy.

#### 1.5.1. Organization responsible for administrating the document

Asseco Data Systems S.A.
PL 80-864 Gdańsk, Jana z Kolna Street 11
National Court Register no: 0000421310 District Court in Gdańsk-North in Gdańsk

#### 1.5.2. Contact

Asseco Data Systems S.A.
Certum
PL 71-838 Szczecin, Bajeczna Street 13
E-mail: infolinia@certum.pl
Phone: +48 91 4801 340

#### 1.5.3. Entities determining the validity of the principles contained in the document

The validity and usefulness of this RQSCD Policy is assessed on the terms described in the Main Policy.

#### 1.5.4. Approval Procedures

Approval procedure of this RQSCD Policy takes place according to the rules described in the Main Policy.

### 1.6. Definitions and abbreviations

The scope related to this chapter was addressed in the Main Policy, and specific definitions for the RQSCD Policy can be found at the end of this document.

## 2. Publication and Repository

### 2.1. Repository

The scope related to this chapter was addressed in the Main Policy.

### 2.2. Information Published by Certum

The scope related to this chapter was addressed in the Main Policy.

### 2.3. Frequency of Publication

The frequency of publication of this RQSCD Policy takes place on the same terms as the frequency of publication of the Main Policy, which was described in the Main Policy in chapter 2.3.

### 2.4. Access to Publications

The scope related to this chapter was addressed in the Main Policy.

## 3. Identification and Authentication

### 3.1. eID means or identity linking

The scope of this item is addressed in Chapter 3 of the Master Policy.

Each signer must be properly authenticated and identified to perform any operation using the key.

The identity of a legal entity is verified during the customer registration process in the qualified services registration system. Client identification is performed in accordance with Article 24.1 of the *eIDAS Regulation* and is carried out at a high level of assurance (Level of Assurance High) or with a high level of confidence as defined in Article 24.1a(c) (High Level of Confidence) of the *eIDAS Regulation*.

The application for access to the service and customer registration takes place during the registration process for the service of issuing a qualified signature certificate or a qualified seal certificate.

The electronic identification means issued as part of the IdP/CAS service meets the requirements for a high level of confidence or a high degree of assurance in accordance with Article 24.1a of the *eIDAS Regulation*, both in terms of the level of data reliability and the mechanisms for releasing such data.

The service unambiguously links the keys used for signing to the reference identifier of the electronic identity means that identifies the customer by assigning a cryptographic card containing those keys to the customer.

As part of its service for managing qualified signature/seal creation devices, Certum uses:

- internal authentication services,
- external authentication services integrated into the identification scheme used by the European Digital Identity Wallet (mObywatel).

### 3.2. Link to the certificate

The scope related to this chapter was addressed in the Main Policy.

### 3.3. Issuance of electronic identification means

The signature activation data is set by the subscriber for long-term certificates.

Data used to generate the electronic identification token and activate the private key is provided to the user as follows:

- OTP generator's SEED – generated by Certum and transmitted to the SimplySign mobile app after the user is authenticated using their credentials,
- OTP generated based on the SEED and the current time using the SHA-2 algorithm and transmitted to the application for authentication by the end user,
- PIN for key activation – set exclusively by the customer during the application process for a qualified signature or seal certificate.

Activation of the signature operation using a certificate issued during the signing process is performed by the service recipient, who maintains control over the entire process by having exclusive control over their mobile phone:

- via a push notification after authenticating in the mObywatel app (the official government mobile app that allows secure identity verification);

- an authorization code will be sent via SMS to this phone, allowing the user to use the private key stored in the hardware cryptographic module to sign the document.

## 3.4. Other services

### 3.4.1. Operational characteristic

#### 3.4.1.1 Certificate status services

The scope related to this chapter was addressed in the Main Policy.

#### 3.4.1.2 Electronic timestamp service

The scope related to this chapter was addressed in the Main Policy.

#### 3.4.1.3 Qualified Validation and Preservation Service for qualified electronic signatures and qualified electronic seals

The scope related to this chapter was addressed in the Main Policy and in the Policy for the Validation and Preservation of Qualified Electronic Signatures and Qualified Electronic Seals.

#### 3.4.1.4 Qualified electronic registered delivery service

The scope related to this chapter was addressed in the Main Policy and in Policy for electronic registered delivery service.

### 3.4.2 Services availability

The scope related to this chapter was addressed in the Main Policy.

### 3.4.3 Optional functions

Not applicable.

## 3.5 End of subscription

Not applicable.

## 3.6 Key escrow and restoration

The scope related to this chapter was addressed in the Main Policy.

### 3.6.1 Principles and of key escrow and restoration

Not applicable.

### 3.6.2 Session key encapsulation, restoration policy and practice

Not applicable.

# 4. Facilities, Management and Operational Controls

This chapter describes general requirements concerning control, physical and organizational security, as well as personnel activity, used in Certum mainly in the time of key generation, entity authenticity verification, certificate and trust service providers certificate issuance and publication, certificate and trust service providers certificate revocation, audit and backup copy creation.

### 4.1. Physical security controls

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.1. Site location and construction

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.2. Physical access

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.3. Power and air conditioning

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.4. Water exposure

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.5. Fire prevention

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.6. Media storage

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.7. Waste disposal

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.8. Offsite backup storage

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.9. Registration authority security controls

The scope related to this chapter was addressed in the Main Policy.

##### 4.1.9.1. Site location and construction

The scope related to this chapter was addressed in the Main Policy.

##### 4.1.9.2. Physical access

The scope related to this chapter was addressed in the Main Policy.

##### 4.1.9.3. Power and air conditioning

The scope related to this chapter was addressed in the Main Policy.

##### 4.1.9.4. Water exposure

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.9.5. Fire prevention and protection

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.9.6. Media storage

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.9.7. Waste disposal

The scope related to this chapter was addressed in the Main Policy.

#### 4.1.9.8. Offsite archive storage

The scope related to this chapter was addressed in the Main Policy.

### 4.1.10. Service recipient security

Service recipient is responsible for the security of signature activation data.

## 4.2. Organizational security controls

The scope related to this chapter was addressed in the Main Policy.

### 4.2.1. Trusted roles

The scope related to this chapter was addressed in the Main Policy.

### 4.2.2. Numbers of persons required per task

The scope related to this chapter was addressed in the Main Policy.

### 4.2.3. Identification and Authentication for Each Role

The scope related to this chapter was addressed in the Main Policy.

### 4.2.4. Roles that cannot be combined

The scope related to this chapter was addressed in the Main Policy.

## 4.3. Personnel controls

The scope related to this chapter was addressed in the Main Policy.

### 4.3.1. Qualifications, experience and authorization

The scope related to this chapter was addressed in the Main Policy.

### 4.3.2. Personnel verification procedure

The scope related to this chapter was addressed in the Main Policy.

### 4.3.3. Training requirements

The scope related to this chapter was addressed in the Main Policy.

#### 4.3.4. Retraining Frequency and Requirements

The scope related to this chapter was addressed in the Main Policy.

#### 4.3.5. Job rotation

The scope related to this chapter was addressed in the Main Policy.

#### 4.3.6. Sanctions for Unauthorized Actions

The scope related to this chapter was addressed in the Main Policy.

#### 4.3.7. Contract Personnel

The scope related to this chapter was addressed in the Main Policy.

#### 4.3.8. Documentation Supplied to Personnel

The scope related to this chapter was addressed in the Main Policy.

### 4.4. Events recording, security incidents management and audit procedures

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.1. Types of events recorded

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.2. Frequency of event logs checking

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.3. Event journals retention period

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.4. Protection of event logs

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.5. Procedures for event logs backup

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.6. Collecting data for internal and external audit

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.7. Notification to event responsible entities

The scope related to this chapter was addressed in the Main Policy.

#### 4.4.8. Vulnerability assessment

The scope related to this chapter was addressed in the Main Policy.

### 4.5. Records archival

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.1. Types of data archived

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.2. Archive retention period

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.3. Archive protection

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.4. Backup procedures

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.5. Requirements for electronically timestamping of the records

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.6. Collecting of archival data (internal and external)

The scope related to this chapter was addressed in the Main Policy.

#### 4.5.7. Procedures to obtain and verify archive information

The scope related to this chapter was addressed in the Main Policy.

### 4.6. Key changeover

The scope related to this chapter was addressed in the Main Policy.

### 4.7. Key security violation and disaster recovery

The scope related to this chapter was addressed in the Main Policy.

#### 4.7.1. Procedures for handling incidents and respond to threats

The scope related to this chapter was addressed in the Main Policy.

#### 4.7.2. Computing resources, software, and/or data are corrupted

The scope related to this chapter was addressed in the Main Policy.

#### 4.7.3. Key compromise or suspicion of certification authority private key compromise

The scope related to this chapter was addressed in the Main Policy.

#### 4.7.4. Business continuity capabilities after a disaster

The scope related to this chapter was addressed in the Main Policy.

### 4.8. Certification authority termination or service transition

The scope related to this chapter was addressed in the Main Policy.

#### 4.8.1. Requirements associated with duty transition

The scope related to this chapter was addressed in the Main Policy.

#### 4.8.2. Dealing with a terminated certification authority

The scope related to this chapter was addressed in the Main Policy.

## 5. Technical Security Controls

This chapter describes procedures for generation and management of cryptographic keys pairs of Certum and users, along with the accompanying technical conditions.

### 5.1. Key pair generation and installation

#### 5.1.1. Key pair generation

##### 5.1.1.1. The environment and the cryptographic module

The environment and the cryptographic module used to store private keys meet the requirements set forth in chapter 6.2.1 of the Main Policy.

##### 5.1.1.2. Algorithms and Key Lengths

Cryptographic keys are generated in a cryptographic module that meets the requirements of FIPS 140-2 Level 3 or higher, using the RSA algorithm, for key lengths of 3072 and 4094 bits. Key lengths and algorithms are updated in accordance with ETSI TS 119 312 (recommended key sizes vs. time) and the requirements of SOG-IS-CRYPTO and ECCG/ENISA in the specification: "Agreed Cryptographic Mechanisms."

##### 5.1.1.3. Key protection

Implemented in accordance with HSM's specifications regarding the storage of data related to cryptographic keys.

##### 5.1.1.4. HSM initialization

The HSM is initialized in accordance with the HSM Management Procedure.

##### 5.1.1.5. Public and private key generation

Private keys (as well as public keys) can be in one of three basic states (according to the ISO/IEC 11770-1 standard):

- awaiting activity (ready) – the key has already been generated but is not yet available for use (the current date of the certificate associated with this key is earlier than the start date of the certificate's validity period), or a key that has not yet been associated with a certificate,
- active – the key can be used in cryptographic operations (e.g., for creating electronic signatures or seals), and the current date falls within the validity period of the associated certificate, and the certificate has not been revoked,

- dormant – in this state, the key may be used exclusively for decryption operations (the subscriber cannot use the private key to create an electronic signature or seal) – the certificate has expired.

#### 5.1.1.6. Procedures of generation of Certum initial keys

The scope related to this chapter was addressed in the Main Policy.

#### 5.1.1.7. Certification authority keys re-key procedures

The scope related to this chapter was addressed in the Main Policy.

### 5.1.2. Delivery of the private key to the end user and methods for activating the private key

Subscribers' keys are generated by the certification authority in the hardware cryptographic module (HSM) and are made available remotely to the subscriber.

Certum allows subscribers to use the keys only in certified devices entered on the list of certified devices for creating qualified signatures and qualified seals, notified in accordance with sec. 30(2), sec. 39(2), and sec. 39(3) of eIDAS Regulation.

Qualified service subscribers receive access to personalized virtual cards placed on a cryptographic hardware module. Card personalization involves preparing the card for use, i.e., generating a unique card number and a unique key pair. The card created in this way serves as a secure device that will store the subscriber's certificate.

Card activation data:

- set by the subscriber in the case of cards stored on an HSM device; the subscriber sets the PIN and PUK codes after receiving the certificate associated with the key pair on the card,
- code sent via SMS, which is required to create an electronic signature, is provided to users separately during the signing process for certificates with a short validity period (up to and including 24 hours) issued during the signing process,
- via PUSH notifications after authentication in the mObywatel app (the official government mobile app that allows for secure identity verification)for certificates issued during the signing process, with a short validity period (up to and including 24 hours).

Certum guarantees that the procedures employed in certificate authority at no time after private key generation do not allow it to be used for creation of electronic signature, nor do they create conditions that will enable the creation of such a signature by another entity, apart from the owner of the key.

Interruption of the signing process after certificate issuance results in the removal of the private key, which makes it impossible to create signature with the use of this key.

For one-time signatures, users' private keys are activated only after authentication (by entering a code received via SMS or push notification) and only for the duration of the electronic signature process using that key. Once the operation is complete, the private key is automatically deleted from the hardware cryptographic module.

Private key can't be used to sign or seal a document if the certificate is invalid, revoked, or suspended.

Private keys may only be used with the signer's consent after the activation method has been initiated.

### 5.1.3. Public Key Delivery to certification authority

Not applicable.

### 5.1.4. Certification authority public key delivery to relying parties

The scope related to this chapter was addressed in the Main Policy.

### 5.1.5. Key Usage Purposes

The algorithms used to generate signatures and seals are SHA-256, SHA-384, and SHA-512. Throughout the entire validity period of the signing certificate, we verify the use of algorithms recommended by ETSI TS 119 312, SOG-IS-CRYPTO, and ECCG/ENISA in the specification: "Agreed Cryptographic Mechanisms."

## 5.2. Private key protection

Service recipient's keys are generated and maintained in a hardware cryptographic module. Certification authority (see chapter 5.1.1. Key pair generation ), which generates the key pair on behalf of the service recipient, must securely provide access to the key pair and instruct the service recipient on the principles of private key protection (see chapter 5.1.2. ).

### 5.2.1. Standards for Cryptographic Modules

The scope related to this chapter was addressed in the Main Policy.

### 5.2.2. Private Key Multi-Person Control

The scope related to this chapter was addressed in the Main Policy.

#### 5.2.2.1. Acceptance of secret shares by its holders

The scope related to this chapter was addressed in the Main Policy.

#### 5.2.2.2. Protection of secret shares

The scope related to this chapter was addressed in the Main Policy.

#### 5.2.2.3. Availability and erasure (transfer) of shared secret

The scope related to this chapter was addressed in the Main Policy.

#### 5.2.2.4. Responsibilities of shared secret holder

The scope related to this chapter was addressed in the Main Policy.

### 5.2.3. Private Key Escrow

Subscribers' private keys are stored on a hardware cryptographic module and are accessible only to the subscriber after authentication (by entering a PIN), and for certificates issued during the signing process, after entering a code received via SMS or a push notification in the mObywatel app.

### 5.2.4. Private Key Backup

The scope related to this chapter was addressed in the Main Policy.

Certum does not retain copies of service recipients private keys.

### 5.2.5. Private Key Archival

The scope related to this chapter was addressed in the Main Policy.

### 5.2.6. Private Key Entry into Cryptographic Module

The scope related to this chapter was addressed in the Main Policy.

### 5.2.7. Private Key Storage in Cryptographic Module

Depending on cryptographic module type private keys can be stored in the module in plain or encrypted form. Regardless of private key storing form it is not accessible from outside cryptographic module for unauthorized entities.

### 5.2.8. Methods of Deactivating Private Key

Not applicable.

### 5.2.9. Methods of Destroying Private Key in a remote signature or seal service

The scope related to this chapter was addressed in the Main Policy.

#### 5.2.9.1. Removal of the key used to create signature or seal

When a signature or seal certificate expires, the keys associated with that certificate are automatically destroyed by the remote signature or seal service. When a subscriber revokes a signature or seal certificate, the keys associated with that certificate are automatically destroyed by the remote signature or seal service. The subscriber can request the destruction of their keys using the provided SimplySign Desktop software for Windows.

Completing the signing process with the certificate issued in the signing process results in the private key being deleted, which prevents the use of that key to create another signature.

Interrupting the signing process after a certificate has been issued in the signing process results in the private key being deleted, which prevents the creation of a signature using that key.

Key destruction is performed as a standalone operation in a single session and is not combined with a signing or sealing operation (except for the keys of certificates issued in the signing process).

#### 5.2.9.2. Removal of the key used to create signature or seal by destroying the cryptographic module

An action performed by the remote signature or seal service results in the deletion of all subscribers' keys stored on the HSM hardware module.

### 5.2.10. Cryptographic Modules ratings

The scope related to this chapter was addressed in the Main Policy.

## 5.3. Other Aspects of Key Pair Management

The scope related to this chapter was addressed in the Main Policy.

### 5.3.1. Public Key Archive

The scope related to this chapter was addressed in the Main Policy.

### 5.3.2. Usage Periods of Public and Private Keys

The scope related to this chapter was addressed in the Main Policy.

Validity period of the certificate issued in the signing process is no longer than 1 day.

## 5.4. Activation Data

Signature activation data is used to activate private keys used by registration authorities, certification authorities and service recipients. They are used at the moment of subject authentication and access control to the private key.

### 5.4.1. Activation Data Generation and Installation

Signature activation data is set by the subscriber for long-term certificates.

Activation of the signature using a certificate issued during the signing process is performed by the user, who maintains control over the entire process by having exclusive control over their mobile phone:

- via PUSH notification after authentication in the mObywatel app (the official government mobile app that allows for secure identity verification),
- user will receive an SMS on that phone containing a code authorizing the use of the private key stored in the hardware cryptographic module to sign the document.

### 5.4.2. Other Aspects of Activation Data

The authorization code cannot be changed.

## 5.5. Computer Security Controls

The scope related to this chapter was addressed in the Main Policy.

## 5.6. Technical control

The scope related to this chapter was addressed in the Main Policy.

## 5.7. Network Security Controls

The scope related to this chapter was addressed in the Main Policy.

## 5.8. Electronic Timestamps as a security control

The scope related to this chapter was addressed in the Main Policy.

## 6. Certificate, CRL, and OCSP Profile

All certificate profiles, trust service provider certificates, certificate status token (OCSP token) are included in the Main Policy. This Policy contains only those elements of profile of the certificate issued during the signing process, that are specific for this profile. Certificates are issued by the Certum QCA 2017 and Certum QCA G3 R35 authority.

Profile of qualified certificates of electronic signature issued in the signing process comply with the format described in ITU-T X.509 v.3 and profiles included in the ETSI EN *319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5*.

## 7. Compliance audit

The scope related to this chapter was addressed in the Main Policy.

## 8. Other Business and Legal Matters

The scope related to this chapter was addressed in the Main Policy.

In addition, it should be noted that all business matters related to the issuance of certificates (specifically, certificates where the keys are managed remotely by the service) are settled between Asseco Data Systems S.A. and BPPT or the Business Partner at the time of signing.

### 8.1. Fees

The scope related to this chapter was addressed in the Main Policy.

### 8.2. Financial Responsibility

The scope related to this chapter was addressed in the Main Policy.

### 8.3. Confidentiality of business information

The scope related to this chapter was addressed in the Main Policy.

### 8.4. Privacy of Personal Information

The scope related to this chapter was addressed in the Main Policy.

### 8.5. Intellectual Property Rights

The scope related to this chapter was addressed in the Main Policy.

### 8.6. Commitments and guarantees

The scope related to this chapter was addressed in the Main Policy.

### 8.7. Warranty Disclaimer

The scope related to this chapter was addressed in the Main Policy.

### 8.8. Liability

The scope related to this chapter was addressed in the Main Policy.

### 8.9. Compensations

The scope related to this chapter was addressed in the Main Policy.

### 8.10. Certificate Policy and Certification Practice Statement validity period

This Policy on the Provision of Qualified Trust Service "Management of remote electronic signature/seal creation devices" is effective from the date specified as its effective date until the publication of the next updated version. Interested parties may submit comments on the proposed changes within 7 business days from the date of their announcement (as described in Section 9.12 of the Master Policy). After this period, if there are no significant objections regarding the substantive content of the proposed changes, the new version of the This Policy on the Provision of Qualified Trust Service "Management of remote electronic signature/seal creation devices" becomes effective as of the validity date specified therein. The decision to approve the new version of the Policy is made by Certum's management. All changes made to the document are recorded in the Document History.

### 8.11. Users notification and communication

The scope related to this chapter was addressed in the Main Policy.

### 8.12. Change introduction procedure

The scope related to this chapter was addressed in the Main Policy.

### 8.13. Disputes Resolution, complaints

The scope related to this chapter was addressed in the Main Policy.

### 8.14. Governing law

The scope related to this chapter was addressed in the Main Policy.

### 8.15. Accordance with applicable law

The scope related to this chapter was addressed in the Main Policy.

### 8.16. Other laws

The scope related to this chapter was addressed in the Main Policy.

### 8.17. Additional provisions

#### 8.17.1. Other Certum Policies

This Policy is a document that bases and supplements the "Certification Policy and Certification Practice Statement of Certum Qualified Services".

Certum also provides other qualified services; the scope of these services is outlined in the Main Policy.

## 9. Document History

| Document modification history | | |
|---|---|---|
| 1.0 | March 15, 2026 | Preparation of the document. |

## 10. Glossary

**Acceptance code -** a code sent by SMS, the introduction of which means acceptance of certificate issued in accordance with the information contained in the Statement.

**Business Identity Confirmation Point (BICP)** - its function is to validate and confirm the service recipient's identity in the process of issuing qualified signature certificates in the process of signing documents (usually contracts) for the needs of the service provided by the organization responsible for the Business Identity Confirmation Point. BPPT are points operating within registration points next to the group of Identity Confirmation Points (e.g. banking or leasing facilities), the nature, scope and openness of operation of which depends on the adopted business model between Certum and a given Business Partner.

**Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service - certificate issued in the signing process (CISP Policy)** - this document bases and supplements the "Certification Policy and Certification Practice Statement of Certum Qualified Services", referred to as the Main Policy, which defines the general rules applied by Certum during the provision of qualified trust services. This document also acts as a Certification Policy for each type of qualified certificates and for the service of issuing qualified certificates in the signing process, including registration of service recipients and certification of public keys.

**eIDAS Regulatio**n – Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, together with Regulation (EU) No 2024/1183 of the European Parliament and of the Council (EU) 2024/1183 of April 11, 2024, amending Regulation (EU) No. 910/2014 with regard to the establishment of a European Digital Identity Framework.

**Issuing a certificate in the signing process -** In order to complete the business process with a Business Partner, it is necessary to sign the documents by the parties - the Business Partner and his client. For this purpose, for the purpose of signing a document (or a package of documents), a certificate with a short validity period is issued, associated with a private key, which will be used to create signatures only as part of the business process being processed. It will not be possible to use this key to sign documents other than those presented to the client for review and intended for signature during the signing process.

**Signature authorizing code -** a code sent via SMS, the introduction of which authorizes the use of the private key contained in the hardware cryptographic module (HSM) to create an electronic signature. When using the mObywatel app, the authorization code may be sent as a push notification to the mObywatel app.