Policy and Practice Statement of Certum eDelivery Qualified Service – electronic registered delivery

Version 1.1

Valid from: February 26th, 2024

Asseco Data Systems S.A.
ul. Jana z Kolna 11
80-864 Gdańsk
www.assecods.pl

Certum
ul. Bajeczna 13
71-838 Szczecin
www.certum.pl
www.certum.eu

Clause: Copyright

Certum is the registered trademark of Asseco Data Systems S.A. Certum and Asseco Data Systems S.A. logo are Asseco Data Systems S.A. trademarks and service marks. Other trademarks and service marks mentioned in this document are the property of their respective owners. Without a written permission of Asseco Data Systems S.A. it is prohibited to use these marks for any purpose other than for information purposes, i.e. it is prohibited to use this marks to obtain financial benefit or compensation in any form.

Asseco Data Systems S.A. hereby reserves all rights to the publication, created products and any parts thereof under civil and commercial law, in particular copyrights, related rights and trademarks.

Without limiting the rights reserved above, no part of this publication may be reproduced or distributed in retrieval systems or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) or otherwise exploited for commercial purposes, without the prior written permission of Asseco Data Systems S.A.

Notwithstanding the above conditions, permission is granted to reproduce and distribute this document on a royalty-free basis, provided that the following copyright notice is clearly displayed at the beginning of each copy and the document is reproduced in its entirety with a note stating that it is the property of Asseco Data Systems S.A.

All the questions concerning copyrights shall be addressed to Asseco Data Systems S.A., Jana z Kolna 11 Street, 80-864 Gdańsk, Poland, e-mail: infolinia@certum.pl.

Table of contents

1. Introduction

The "Policy and Practice Statement of Certum eDelivery Qualified Service – electronic registered delivery" hereinafter referred to as the eDelivery Policy is a document based on and complementary to the "Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services" hereinafter referred to as the **Master Policy**, which sets out the general principles applied by Certum when providing qualified trust services. This document also serves as a Policy for the eDelivery trust service, covering the registration of customers and the process of identifying entities using the service.

The above service is provided in accordance with:

- the implemented by Asseco Data Systems S.A. Integrated Management System, which includes in particular the requirements of the PN-EN ISO 9001 and PN-ISO/IEC 27001 standards,
- *Polish Act on Trust Services and Electronic Identification of 5 September 2016 (OJ of 2021, item 1797, as amended died) as amended*,
- *Polish Electronic Delivery Act of 18 November 2020*,
- *Polish Regulation on preparing and delivering electronic documents and making available forms, templates and copies of electronic documents (Journal of Laws 2011 No. 206, item 1216), as amended;*
- *Regulation No. 910/2014 of the European Parliament and of the Council (EU) on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC, hereinafter referred to as the eIDAS Regulation;*
- *ERD Service Standard – the standard for a public electronic registered delivery service provided by a designated operator and qualified trust service providers providing qualified electronic registered services for interaction with a public registered electronic delivery service and inbox*.

This eDelivery and Master Policy also define the participants in the process, their duties and responsibilities, identity verification procedures, and application areas. Knowing the nature, purpose, and role of Policies is especially important from the perspective of the customer.

The structure and substantive content of the eDelivery Policy are consistent with Recommendation RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. It also meets the requirements of the following standards:

- *ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;*
- ETSI EN 319 521– *Electronic Signatures and Infrastructures (ESI); Policy and security for Electronic Registered Delivery Service Providers.*

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

1.1. Introduction

The eDelivery Policy describes the scope of Certum (operating within Asseco Data Systems S.A.) operations and its associated **registration points, customers**. It also defines the general rules for the provision of eDelivery qualified trust service, in accordance with the *Polish Act on Trust Services and Electronic Identification of 5 September 2016 (OJ of 2021, item 1797, as amended died),* hereinafter referred to as the *Act*, i.e. **the standard of the service of electronic registered delivery** including registration of customers, technical requirements for the transmission of electronic documents, the **method of identification of the sender and addressee**, the structure as well as the form and method of issuing proofs of sending and receiving as well as recording, the scope and structure of data on communication between addresses for electronic delivery, the requirements for the operation of the inbox.

Certum **providing** the qualified eDelivery service shall provide the service based on the certificate of trust service providers issued by the minister responsible for information technology or a trust service provider authorized by him/her pursuant to Article 10(1) of *the Polish Act on Trust Services and Electronic Identification*. Trust Service Provider is the **National Certification Center being an IT system of the National Bank of Poland**.

This document governs the operation of the **eDelivery** service and its associated registration points, as well as customers of this service, using the service or exchanging any messages with the service.

The scope related to other trust services provided by Certum is addressed in the Master Policy.

Certum acts in accordance with the law applicable in the Republic of Poland and the rules resulting from the observance, construction, interpretation and validity of the eDelivery Policy.

Related to the eDelivery Policy are the Terms & Conditions of Certum eDelivery Qualified Service – electronic registered delivery and other additional documents that Certum is obliged to use in its operation. These documents are listed in the Master Policy.

Certum is responsible for compliance with the procedures described in this document.

Additional information and service support can be obtained via email at: infolinia@certum.pl.

The scope of other services related to this item is addressed in the Master Policy.

1.2. Document name and identification

This document is assigned a proper name of the following form: **Policy and Practice Statement of Certum eDelivery Qualified Service – electronic registered delivery** and is available in electronic form on the website of the Certification Authority available at www.certum.pl.

The following registered object identifiers are associated with the above document:

(OID: 1.2.616.1.113527.2.4.1.0.4.1.1)[1]:

> **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)(4) version(1) 1}**

where the last two numerical values refer to the current version and subversion of this document.

[1] eDelivery Policy and Practice Statement document identifier.

1.3. eDelivery Policy Parties

This document and the Master Policy govern all major relationships between the entities comprising Certum, its advisory teams (including auditors) and its clients (users of the services provided). Specifically, these regulations address:

- authorities,
- Primary Registration Points (PRP),
- registration points (RP),
- persons confirming the identity,
- customers,
- relying parties.

Certum provides trust services to all natural persons, legal entities or entities without legal personality, accepting the regulations of the present document and the Master Policy.

Certum **in its operation shall ensure that none of its clients or relying parties is directly or indirectly treated less favorably than others, or restricted in the exercise of their rights, on the grounds of age, color, religion, disability, ethnic or national origin, sex, marital status, physical health, mental health, nationality, physical appearance or political opinion**.

Certum **has specific procedures in place to handle blind and visually impaired individuals applying for access to the service.**

Certum provides a qualified eDelivery service for:

- registration of customers,
- identification of the sender and addressee,
- "indication of authorized user",
- creating an electronic delivery address,
- activation of electronic delivery address,
- updating the entry in the BAE registry,
- request to the removing electronic delivery address from the BAE registry,
- extending the validity of the electronic delivery address entry in the BAE registry,
- recovering deleted electronic delivery address,
- transferring your electronic delivery address to another provider,
- sending messages and attached documents/files
- providing evidence related to the data being transmitted.

1.3.1. Trust Service Authorities

Qualified Certum eDelivery service provided by Certum QERDS 2023.

Other authorities, services included in Certum **providing qualified trust services** are defined in the Master Policy.

1.3.1.1. Certum qualified eDelivery service

The Certum eDelivery qualified electronic registered delivery service operates on the basis of registration of Asseco Data Systems S.A. in the register of qualified trust service providers. The Certum eDelivery service is supervised by the minister responsible for digitization or an entity indicated by him/her (the national certification center).

The Certum eDelivery qualified electronic registered delivery service provides the ability to electronically send and receive correspondence, evidence related to the data being transmitted, including proof of sending and receiving the data, protect the data being transmitted from the risk of loss, theft, damage or any unauthorized alteration. By initial identification the sender and recipient, it ensures that messages are not delivered to an unauthorized user.

A qualified eDelivery service provides a qualified time-stamping and security with a qualified seal for sending, receiving and any changes to correspondence.

The evidence contains information that a certain event took place at a specific point in time.

The **Certum eDelivery** service provides services for:

- natural persons, legal entities and entities without legal personality.

1.3.2. Primary Registration Authority, Registration Points and Identity Confirmation Points

The Certum eDelivery service closely cooperates with the Primary Registration Authority, registration points and identity confirmation points. Registration points and identity confirmation points represent Certum eDelivery in their relations with customers and act within the scope of their authority to register customers and confirm their identity.

Registration points and identity confirmation points accept, verify and approve or reject – received from applicants – applications for service registration and other applications related to service management. Applications are verified in order to authenticate (based on the documents attached to the application) the applicant and the data that has been included in the application. The degree of accuracy in confirming the identity of the customer and the attributes attributed to the customer is based on the general requirements specified in the **eDelivery Policy** (see chapter 3.2). The detailed scope of responsibilities of registration points, identity confirmation points and their operators is defined by this eDelivery Policy, the Master Policy on the procedures of operation of registration points, identity confirmation points and the Terms & Conditions of Certum eDelivery Qualified Trust Service – electronic registered delivery.

The remaining scope related to this item is addressed in the Master Policy.

1.3.3. Customer

Customers of Certum may be natural persons, legal entities or entities without legal personality.

Organizations wishing to obtain access to the service for their employees may do so through their authorized representatives. An individual customer, on the other hand, applies for access to the service on his/her behalf[2].

Customers may use the eDelivery service as senders and/or addressees.

1.3.4. Relying parties

The relying party using the service is any entity that makes a decision about its evidential validity.

In this case, they are not users of the eDelivery service.

[2] Regardless of whether the customer applies for access to the service individually or an authorized representative does it on his/her behalf, obtaining access to the service must be preceded by the customer's acceptance of the terms of eDelivery services by Asseco Data Systems S.A.

1.3.5. Other Parties

Independent bodies that assess compliance with the eIDAS Regulation.

A supervisory authority, i.e. the minister responsible for digitization or an entity designated by him/her **(national certification center**).

1.4. Scope of application of the eDelivery electronic registered delivery service

The eDelivery service is used to send and receive electronic message.

Electronic registered delivery provides electronic proof that an electronic document has been sent by the sender to the addressee, and ensures that the message transmitted is protected from the risk of loss, theft, damage, or any unauthorized alteration.

Other services included in Certum **providing qualified trust services** are defined in the Master Policy.

1.4.1. eDelivery Trust Service Provider Certificate

The eDelivery Trust Service Provider Certificate is issued only by the minister responsible for digitization or a qualified trust service provider authorized by him/her.

1.4.2. Non-recommended use of the eDelivery service

It is forbidden to use the eDelivery service in violation of the applicable regulations and contrary to the purpose specified herein.

1.5. Administration of the Certification Practice Statement

Administration of this eDelivery Policy shall be as described in the Master Policy.

1.5.1. Organization responsible for administration of the document

Asseco Data Systems S.A.
Jana z Kolna 11 Street
80-864 Gdańsk
Poland
KRS: 0000421310 District Court Gdańsk-Północ in Gdańsk

1.5.2. Contact

Asseco Data Systems S.A.
Certum
Bajeczna 13 Street
71-838 Szczecin
Poland
E-mail: infolinia@certum.pl
Phone no.: +48 91 4801 340

1.5.3. Entities that determine the validity of the principles set out in the document

Evaluation of the validity and relevance of this eDelivery Policy shall be carried out on the basis described in the Master Policy.

1.5.4. Procedure for Approval of the Policy and Practice Statement of Certum Qualified Service

Evaluation of the validity and relevance of this eDelivery Policy shall be carried out on the basis described in the Master Policy.

1.6. Definitions and abbreviations used

The scope associated with this item is addressed in the Master Policy, while definitions specific to this eDelivery Policy can be found at the end of this document.

2. Responsibility for publication and repository

2.1. Repository

The scope related to this item is addressed in the Master Policy.

2.2. Information published in the repository

The scope related to this item is addressed in the Master Policy.

On the www.certum.pl website in the repository, the Certum eDelivery qualified trust service providers certificate, which is not expired or revoked, can also be found.

2.3. Frequency of publication

The frequency of publication of this eDelivery Policy follows the same rules as the frequency of publication of the Master Policy which are described in the Master Policy in chapter 2.3.

2.4. Repository access control

The scope related to this item is addressed in the Master Policy.

3. Electronic delivery address, identification and authentication of customers

There are general rules to verify identity of clients that can be used by Certum, as shown below.

Verification is **mandatory** during registration.

Certum and its subordinate entities shall confirm the identity and any special attributes of the natural person or legal entity applying for access to the service on the basis of a valid identity card, mDowód document[3], passport, polish residency card or using another method subject to Article 44 *of the eIDAS Regulation*.

3.1. Electronic delivery address

3.1.1. Electronic delivery address structure

An electronic delivery address is created as a string of characters to ensure its uniqueness.

An electronic delivery address does not explicitly or implicitly include information regarding the name or other identifier of the subject.

The electronic delivery address shall be structured in accordance with the requirements specified in [ETSI319412-1] in chapter 5.1 as follows:

- For natural persons in the form of a semantic identifier id-etsi-qcs-SemanticsId-Natural;
- For public and non-public entities in the form of semantic identifier id-etsi-qcs-SemanticsId-Legal.

The electronic delivery address has the following structure:

- 3 characters indicating the type of identifier – indicating the electronic address – "AE: ";

[3] Digital ID Card available in mobile application mObywatel issued by Polish Prime Minister's Office.

- 2 characters of the country code in accordance with ISO 3166 standard – denoting Poland – "PL";
- dash "-" – encoded (0x2D (ASCII), U+002D (UTF-8));
- at least 20 characters of a valid electronic address consisting of the following character groups:
    - 5 digit characters (0-9),
    - dash "-" – encoded (0x2D (ASCII), U+002D (UTF-8)),
    - 5 digit characters (0-9),
    - dash "-" – encoded (0x2D (ASCII), U+002D (UTF-8)),
    - 5 letter characters (A-Z – capital letters only),
    - dash "-" – encoded (0x2D (ASCII), U+002D (UTF-8)),
    - 2 digit characters (0-9).

The last 2 characters indicate the checksum.

A sample address following the above structure: "AE:PL-12345-67890-ABCDE-12".

3.1.2. Data identifying the customer

The eDelivery service provides a link between the personal and identification data of senders and addressees, current and historical, and the electronic delivery address supported by the service.

- Data set according to *ETSI EN 319 522-2* for natural persons:
    - first name, last name,
    - place of birth,
    - date of birth,
    - PESEL,
- Data set according to *ETSI EN 319 522-2* for entities other than natural persons:
    - the name of the entity and, in the case of a court enforcement agent, his or her name and title,
    - registered office and address
    - postal address,
    - identification number (NTR,VAT, LEI).

3.1.3. Anonymity of the service

It is required that electronic delivery addresses allow for unambiguous identification of a specific addressee.

3.1.4. The role of trademarks

The scope related to this item is addressed in the Master Policy.

3.2. Initial registration, initial identity verification

Customer registration takes place whenever an application is made for access to the **Certum eDelivery** service and other applications related to the management of the service.

Registration involves a number of internal procedures, which even before granting access to the eDelivery service to the customer, are aimed at collecting, by the registration system point, credible data on the subject, identifying his/her identity and rights. Confirmation of this data is performed in accordance with RDE service standard item 5.1.17.1.

The customer submits an application (declaration), which constitutes confirmation of the truthfulness of his/her data and consent to the assignment of these data to him/her. Based on this application, Certum grants access to the service by assigning authentication means to the sender or the addressee.

The customer is obliged to confirm familiarization with the "Terms & Condions of eDelivery Qualified Trust Service" by accepting the terms of trust services.

The customer is required to provide information in the registration form allowing to identify him/her.

The application for the creation of an electronic delivery address in accordance with *the Polish Electronic Delivery Act* and *ETSI EN 319 522-2* standard includes a data set in the case of natural persons

- first name, last name,
- business name – in the case of a natural person being an entrepreneur entered in the Central Register and Information on Economic Activity (CEIDG), or professional title – in the case of a natural person being an advocate, legal adviser, tax adviser, restructuring adviser, notary public, patent agent or adviser to the Public Prosecutor's Office of the Republic of Poland,
- place of birth,
- date of birth,
- PESEL,
- identification number (NTR, VAT, LEI) – if assigned,
- correspondence address – in case of a natural person who is not an entrepreneur registered in the Central Register and Information on Economic Activity (CEIDG),
- correspondence address – in the case of a natural person who is an entrepreneur entered in the Central Register and Information on Economic Activity (CEIDG)
- e-mail address to which the information about the creation of electronic delivery address and on how to activate the delivery box will be sent,
- where a delivery box administrator is appointed, the name of the delivery box administrator, his or her e-mail address and PESEL.

The application for the creation of an electronic delivery address in accordance with *the Polish Electronic Delivery Act* and *ETSI EN 319 522-2* for entities other than natural persons:

- the name of the entity and, in the case of a court enforcement agent, his or her name and title,
- registered office and address
- postal address,
- identification number (NTR,VAT, LEI),
- the name of the delivery box administrator, his or her e-mail address and PESEL.

Each customer undergoes a registration process. After filling in an electronic application, correct verification of the provided data, after accepting the terms of trust services, he/she receives access to the eDelivery service and receives assigned authentication means.

Each applicant for access to eDelivery services must follow these basic steps:

- complete an electronic application,
- specify the type of service:
  - a non-public entity that is an individual;
  - a non-public entity that is a legal person.

The specific scope of authority to apply for a particular type of service should be defined by a document of title, power of attorney, or other document authorizing to act on someone else's behalf.

During the registration process, the applicant shall be informed in writing or in the form of an electronic document, in a clear and commonly understood manner, of:

- terms of using the eDelivery service,
- obligations of the customer,
- information for relying parties,
- information on the way of data archiving,
- scope and limitations of liability of Asseco Data Systems S.A.,
- scope and limitations of the eDelivery service,
- compliance of the services provided with the *eIDAS Regulation*, *the Act on Trust and Electronic Identification Services and the Act on Electronic Delivery.*
- manner of complaints and disputes handling,
- manner of the eDelivery service auditing,
- Certum's contact information,
- availability of services,
- the procedure for requesting the client to deregister from the eDelivery service.

The above issues are included in the Terms & Conditions of eDelivery Certum Qualified Trust Service – electronic registered delivery available on the website at www.certum.pl.

The customer is obliged to confirm that he/she has read the above information by accepting the terms of the eDelivery service.

Certum guarantees the Polish and English language version of the presented documents, which covers the language area of interest for our clients. The documents presented are downloadable as PDF files through the Certum repository.

Acceptance of the terms of trust services also means that:

- The customer consents to the processing of his/her personal data by Asseco Data Systems S.A. for the purpose of providing the service,
- the customer declares that the information provided by him/her is true and given voluntarily.

When submitting an application, the prospective customer is also required to submit:

- powers of attorney to submit the application on behalf of the authorizing entity,
- other documents that are necessary to confirm the data contained in the application, e.g. a title.

When completing the application, the prospective customer agrees in a statement to:

- processing of his/her personal data by Asseco Data Systems S.A. and the registration system point, for the needs necessary to complete the process.

If the customer has provided a power of attorney, the entity granting the power of attorney shall at the same time be required to sign an additional part constituting the second part of the qualified trust service agreement containing the following elements in accordance with ETSI EN 319 411-1 clause 6.3.4(e):

- consent for the provision of qualified eDelivery services ,
- declaration of acquaintance with the terms of services contained in the Terms & Conditions of eDelivery Qualified Trust Service,
- consent to store the subject's data used in the registration process for the period of time required by the provisions of the *Trust Services and Electronic Identification* Act.

3.2.1. Verification of legal entity's identity – authentication of powers of attorney and other attributes

Verification of powers of attorney takes place whenever a customer applies for access to the service on behalf of an organization whose information is included in the application.

Authentication of powers of attorney or authorizations is a part of processing by the registration point and the certification authority of an application for access to the eDelivery service, representing interests of another legal person.

The power of attorney authentication process used by Certum, in addition to verifying the powers of attorney, also includes authenticating the individual who received the power of attorney or authorization.

The process of confirming powers of attorney involves verifying the power of attorney provided on the basis of:

- submitted authorization documents (e.g. a notarized document of power of attorney granted by a natural person),
- checking if such document was signed by a person authorized to represent,
- checking the compliance of the data of the legal entity included in the application with the submitted documents.

3.2.2. Verification of identity of individuals

Verification of an individual's identity must serve two purposes. First, it must show that the data provided in the application refers to an existing individual, and second that the applicant is indeed the individual named in the application.

In case the customer is a natural person (an employee of the organization or its representative), for whom the access to the eDelivery service is issued, the verification may be additionally performed on the basis of:

- appropriate authorization issued by the organization to represent its interests,
- a valid excerpt from the National Court Register or an excerpt from the entry in the Central Register and Information on Economic Activity (CEIDG);

In case the customer is a natural person (Enforcement Agent, Lawyer or Attorney-at-law), for whom access to the eDelivery service is issued, the verification is additionally carried out on the basis of:

- a document confirming the title held.

The registration inspectors of the Primary Registration Points, the registration point operators, are obliged to verify the correctness and truthfulness of all data provided in the application and concerning the identity of the applicant and his/her powers of attorney (see chapter 4.1).

The procedure for verification of an individual's identity carried out by the registration point operator, the registration inspector of the Primary Registration Point, consists of a detailed verification of the application and documents presented by the customer.

Upon successful completion of the verification procedure, the operator of the registration system or other person verifying identity (except for a notary public) accepts on behalf of Asseco Data Systems S.A. the terms of the eDelivery service, and the application and documents are transferred to Certum in the IT system.

3.2.2.1. Identity verification by an authorized representative of Certum

The confirmation of customer's identity is carried out on the basis of a valid ID card, mDowód document, passport, polish residency card through the Registration Point or Identity Confirmation Point. Confirmation of a customer's identity may take place:

- by personal appearance at the Registration Point or the Identity Confirmation Point,
- through the visit of an authorized Certum representative at the location where the customer is currently residing.

3.2.2.2. Verification of identity based on a qualified electronic signature

Identity verification can be performed remotely, using a valid qualified certificate issued by any Polish provider of qualified trust services. Confirmation of identity is made on the basis of an application bearing a qualified signature of that person.

3.2.3. Customer's information not subject to verification

Certum verifies all information contained in the application.

3.2.4. Verification of authorizations

When an application for access to the service is made on behalf of an organization, this should be interpreted as authorizing the applicant to act on behalf of the organization. At the same time, this means that Certum verifies whether the individual who submitted the application was, at the time of verifying the application, an employee of the organization or an associate of the organization and has the right to act on behalf of the organization; the scope of these rights and the period of their validity may be regulated by separate regulations. Certum verifies the details of the individual and his/her rights based on available records or databases.

If an organization revokes the authorization of an individual requesting access to the eDelivery service, Certum must be notified and a new request must be submitted along with the required authorization.

3.3. Authentication

Authentication of the identity or powers of attorney of customers who already have access to the eDelivery service is performed:

- through assigned authentication means for the sender or addressee, identification is performed each time a message is posted or delivered;
- the message is forwarded only after successful identification of the addressee.

4. Functional requirements

The way in which the eDelivery service is provided is presented below. Each step begins with the customer submitting the appropriate application. Certum makes a decision on the further processing of the application by providing the requested service or refusing to provide it. Submitted applications should include information that is necessary to properly identify the customer and the data contained in the submitted application.

The service allows messages to be sent electronically between individual senders and addressees. This service provides proof of the integrity and time of transmitted data, including proof of sending and receiving. The service protects data against loss, theft, violation of its integrity or unauthorized modification, and meets the requirements of the *eIDAS Regulation*.

When using the eDelivery service, the principle that the legal validity of an electronic document cannot be challenged on the grounds that it is in electronic form is observed to ensure that an electronic transaction is not rejected solely because the document is in electronic form. Therefore, electronic documents sent and received through the eDelivery service are assumed to be comprehensive, sent by the sender and received by the addressee, and that the date and time of sending and receiving are accurate.

4.1. Submission of applications

4.1.1. Who can apply for access to the service

Applications for access to the eDelivery service may be made by any entity that falls into one of the following categories:

- a natural person who is or will be a customer, having a Polish ID (PESEL),
- an authorized representative of a legal entity or institution without legal personality.

Certum does not provide the eDelivery service to minors (under 18 years of age), even if they run a business.

Certum does not grant access to the eDelivery service to entities carrying out their business activity in the countries with which the Republic of Poland law prohibits trade.

4.1.2. Application process and related responsibilities

The application for access to the eDelivery service is submitted by the applicant at the Registration Point, Partner Identity Confirmation Point in person.

4.2. Processing of applications

After the registration system point operator verifies the identity of the applicant (see chapter 3.2.2) and Certum receives the required documents, the application is forwarded to the Primary Registration Point, where a registration inspector prepares a **request –** assignment or transfer from another provider of an electronic delivery address. Having received the delivery address, Certum shall immediately send information on its creation to the e-mail address of the delivery box administrator, if indicated, and in case of a non-public entity being a natural person – also to the e-mail address of the applicant indicated in the application.

4.2.1. Implementation of identification and authentication functions

The functions of identification and authentication of all required customer's data are performed by the Primary Registration Points and cooperating Registration Points and Identity Confirmation Points in accordance with the conditions specified in chapter 1.3.2.

4.2.2. Approval or rejection of the application

4.2.2.1. Application acceptance procedure

The Registration or Identity Confirmation Point accepts and verifies the application for access to the eDelivery service and, together with the required set of documents, forwards it to the Primary Registration Point from where the application is transferred to the BAE (Electronic Address Database) in order to assign a new delivery address or to transfer it from another provider.

4.2.2.2. Refusal to accept the application

Certum may refuse to accept an application from any applicant without incurring any obligation or exposure to any liability which may arise as a result of any loss or expense incurred by the applicant (as a result of the refusal). In such a case, Certum shall reimburse the applicant for the fee for access to the eDelivery service (if the applicant has made a relevant prepayment), unless the applicant has provided false or falsified data in the application for access to the service.

An application may be denied in the following cases:

- the identifier of the customer requesting access to the service overlaps with the identifier of another customer,
- a reasonable suspicion that the customer has falsified or provided false data,

- failure of the applicant to provide a set of required documents constituting an attachment to the application for access to the eDelivery service,
- discovery of handwritten corrections or modifications to submitted formal documents,
- the expiration date of the sent documents has been exceeded – the documents whose signature date has exceeded the deadline of 3 months on the day they were received by Certum in electronic form shall be deemed time-barred,
- the expiration date of the application for access to the service has been exceeded – those applications whose completion date has exceeded the deadline of 3 months as of the date of receipt of Certum in electronic form shall be deemed time-barred,
- other valid reasons not listed above, with prior agreement of the refusal with the **Security Inspector**.

Information on refusal to grant access to the eDelivery service is sent to the applicant in the form of an appropriate decision with a brief justification of the reason for refusal. The applicant may appeal against refusal to Certum within 14 days of receiving the decision.

4.2.3. Waiting period for access to the service

Certum makes every effort to verify the application and grant access to the service as soon as possible after receiving it.

This time depends mainly on the accuracy of the application delivered and any administrative arrangements and clarifications between Certum and the applicant. Waiting time in the BAE (Electronic Address Database), assignment a new address for electronic delivery or transferred from another provider electronic delivery address.

If the reasons that may cause possible delays in granting access to the service are Certum's sole responsibility, such time should not exceed 7 working days from the moment of accepting the terms of the eDelivery service by Asseco Data Systems S.A. and the customer.

4.3. eDelivery service provision process flows

The eDelivery service uses technology that, after the sender is initially identified and authenticated, enables messages and attached documents / files to be sent as parcels. The system used ensures sending messages in a secured and encrypted channel.

Sent and received messages are not scanned by antivirus software

The eDelivery service provides evidence of events that occur during the transmission process (messages, documents, files, and other items) between parties (e.g., information that data was sent by the sender or delivered to the addressee). Such evidence can be used to prove to third parties, and in legal proceedings when necessary, that an exchange of messages or documents occurred at a specific point in time, as evidenced by a qualified time stamp.

Evidence delivered under the eDelivery service are signed with a qualified electronic seal and a qualified time stamp. The proof contains information that at a specific point in time, a specific event occurred related to the data transmission process between the sender and the addressee (e.g. sending or receiving a message). The proof may be delivered immediately to the sender/addressee, but is also kept for a period of 20 years for later access by interested parties in accordance with national legislation.

4.4. Process of providing eDelivery service

The eDelivery service is accessed through a web portal by providing an API. Use of the service requires preliminary identification of the sender and addressee carried out remotely via the mobile application or by personal appearance of these persons or their representatives at the registration system point (see item 3.2). Customers' data collected by Certum includes personal information, contact information, identity document data and more.

The eDelivery service provides the clients to choose one of three options for sending messages from sender to addressee:

- BASIC – normal message – the contents of the message are made available to the addressee without the possibility of rejection.
- CONSENTED – advised message – notification is sent to the addressee before the message is delivered. The addressee is obliged to accept or reject the content of the message; the content of the message is made available only after its acceptance by the addressee.
- CONSENTED SIGNED – as in CONSENTED – with the addition of a signature requirement, a digital signature by the addressee of the acknowledgment of receipt is required.

Messages delivered via the public eDelivery service are only supported in the BASIC option.

The eDelivery service does not provide other options for sending messages from sender to addressee.

The eDelivery service allows the recipient to send an invitation to the eDelivery box to other users.

The user, i.e. the owner of the eDelivery box, independently supervises and allows access to the eDelivery box for other users. Such users are not subject to Certum's supervision. The owner of the eDelivery box is the administrator of the personal data of other users that it maintains in its eDelivery box.

4.5. Identification of the Sender and Addressee

4.5.1. Identification of the Sender

Certum verifies the identity of the sender:

- by the physical presence of a natural person or an authorized representative of a legal entity (in accordance with the representation or under a power of attorney),
- by the qualified certificate.

According to the information contained in point 3.2.

Only after the sender is successfully authenticated, the message is transferred from the system controlled by it to the eDelivery service.

The authentication process takes place in a secure and controlled environment. All evidence of authentication and posting is collected and stored in a protected environment.

4.5.2. Identification of the Addressee

Certum verifies the identity of the addressee:

- by the physical presence of a natural person or an authorized representative of a legal entity (in accordance with the representation or under a power of attorney),
- by the qualified certificate.

According to the information contained in point 3.2.

Only after the addressee is successfully authenticated, the message is forwarded out of the system controlled by it and to the addressee.

The authentication process takes place in a secure and controlled environment. All proof of authentication and receipt of message is collected and stored in a protected environment.

4.6. Gathering evidence

The eDelivery service provides evidence of sending and receiving user content.

Proof of receipt is provided as a separate electronic document in a well-defined format, indicating the exact date and time the addressee received the user content via a qualified time stamp. The proof is electronically signed by the eDelivery authority.

Certum collects and stores data on:

- all events related to the initial verification of the identity of the sender and its identification;
- all events related to the initial verification of the addressee's identity and identification;
- during the initial identity verification, data of a natural person (e.g. ID card, mDowód document, passport, polish residence card), identification data of a legal person (e.g. registration documents, powers of attorney, etc.) and all other data necessary for its correct identification are verified;
- data used to initially identify the sender/addressee;
- service operation data confirming the authentication of the sender and addressee and the communication between them;
- evidence of posting, notification of message, and delivery;
- evidence that the content transmitted by the sender was received by the addressee;
- proof that the content provided by the sender was not altered during transmission;
- Evidence of messages made by other users invited by the service recipient and forwarded to a non-RDE service., Evidence includes data of the service recipient (box owner).

All evidence collected shall be stored in a protected environment.

All evidences are provisioned through:

a) QERDS User Agent – web-based interface of the QERDS service;

b) QERDS API.

Evidences are only provisioned to the QERDS User Agent.

4.6.1. Evidence related to the Sender

The service generates proof of sending, which can also be provided to a third party. The proof shows the exact date and time the content was sent by the sender.

- Acceptance of shipment messages

The sender successfully transfers the message to the eDelivery service.

A proof is generated with a predetermined date and time indicating that the sender, has placed the message via the eDelivery service which has been accepted by the provider and the provider will take all necessary actions to deliver it to the appropriate addressees).

- Rejection of the messages

The sender has transferred the message to the eDelivery service, the message has not been accepted by the service. The generated proof indicates that the sender, handed over the message to the service on the specified date and time, and the eDelivery service refused to perform the necessary actions.

4.6.2. Evidence related to the Addressee

The service generates a proof of receipt, which can also be provided to a third party. The proof shows the exact date and time the content was sent by the sender.

- message delivery

The contents of the message were delivered to the addressee.

Related evidence shows that the message was delivered to the addressee within the established time.

- Failure to deliver message

The message cannot be delivered to the addressee at the agreed time due to technical errors and/or other reasons. There may not be evidence of content delivery within the agreed upon time frame.

Inability to deliver a message can be caused by a variety of events, such as:

- The eDelivery service was unable to send content from sender to addressee.
- While the message was in the eDelivery service, the system, at the specified time, did not receive any proof of successful delivery.

In such cases, evidence of the reason for non-delivery is generated in accordance with the ETSI EN 319 522-1 standard.

4.6.3. In such cases, evidence of the reason for non-delivery is generated. Types of evidence generated

Certum collects and stores the following types of evidence:

- Types of evidence collected for individual events according to *ETSI EN 319 522-1*.

N.	**Event name**
Notification of messages	
A.1	Acceptance of sending messages **(SubmissionAcceptance)**
A.2	Rejection of the messages **(SubmissionRejection)**
Events related to the transfer of a messages between RDE services	
B.1	Acceptance of transfer of messages between RDE services **(RelayAcceptance)**
B.2	Rejecting the transfer of a messages between RDE services **(RelayRejection)**
B.3	Handover error **(RelayFailure)**
Events related to acceptance / rejection by the addressee	
C.1	Notification of acceptance of acceptance **(NotificationForAcceptance)**
C.2	Notification of receipt acceptance error **(NotificationForAcceptanceFailure)**
C.3	Acceptance of preawareness **(ConsignmentAcceptance)**
C.4	Rejection of preawareness **(ConsignmentRejection)**
C.5	Expiration of time to accept/reject messages **(AcceptanceRejectionExpiry)**
Events related to notification of the addressee (pre-awareness) of the arrival of the messages	
D.1	Messages prepared for pickup **(ContentConsignment)**
D.2	Error in preparing messages for collection due to technical error **(ContentConsignmentFailure)**
D.3	Notification of messages ready for pickup **(ConsignmentNotification)**
D.4	Notification error about messages ready for pickup (**ConsignmentNotificationFailure)**
Events related to the delivery of the messages to the addressee	
E.1	Delivery of the messages **(ContentHandover)**
E.2	Error in delivery of messages **(ContentHandoverFailure)**
Events related to connections to systems other than the RDE service	
F.1	Transfer to a non-RDE service **(RelayToNonERDS)**
F.2	Error of transfer to non-RDE service **(RelayToNonERDSFailure)**
F.3	Receipt of messages by non-RDE service **(ReceivedFromNonERDS)**

- Types of evidence collected for each event as required by the Act.

N.	Event name
KP.1	Confirmation of dispatch (**ShipingConfirmation)**
KP.2	Confirmation of receipt (**Delivery Confirmation)**

- Types of internal Certum evidence collected for individual events - not required by the ETSI standard or the Act.

N.	Event name
CE.1	Confirmation of receipt of a package of correspondence (**BatchMessagesRelayConfirmation)**
CE.2	Correspondence package acceptance error (**BatchMessagesRelayFailure)**
CE.3	Statement of intent to receive preawareness (**ConsignmentAcceptanceWillDeclaration)**
CE.4	Statement of intent to reject preawareness (**ConsignmentRemovalWillDeclaration)**
CE.5	Deletion of messages (**ConsignmentRemoval)**

4.7. Protection of transmitted data from the risk of loss, theft, damage or unauthorized modification

Security features for messages are compliant with the RDE service standard.

Other security features see chapter 5.

4.8. Renewal of eDelivery service subscription

Certum provides the option to renew access to the eDelivery service before the box expires.

4.9. Termination of eDelivery service subscription

Certum provides the possibility of removing the electronic delivery address from the BAE registry.

At the end of the provision of the eDelivery service, which allows for communication with public entities (regardless of whether it was reported by the customer or initiated by the system as a result of non-renewal of the subscription), Certum accepts the moment of notifying the BAE register of the desire to resign from handling the ADE address associated with the mailbox, regardless of how the actual process of transferring/deactivating the ADE address in the BAE register itself works.

4.9.1. People who may request termination of the eDelivery service subscription

A request to terminate the eDelivery service subscription, to remove the electronic delivery address from the BAE registry may be submitted by:

- natural person for whom the electronic delivery address has been created,
- legal person – an authorized representative of the legal person, for whom the address for electronic delivery has been created.

5. Technical, organizational and operational security controls

The chapter describes the general requirements for overseeing physical and organizational security controls as well as the activities of the personnel in place at Certum.

5.1. Physical security controls

The scope related to this item is addressed in the Master Policy.

5.1.1. Site location and facility

The scope related to this item is addressed in the Master Policy.

5.1.2. Physical access

The scope related to this item is addressed in the Master Policy.

5.1.3. Power and air conditioning

The scope related to this item is addressed in the Master Policy.

5.1.4. Flooding hazard

The scope related to this item is addressed in the Master Policy.

5.1.5. Fire prevention and protection

The scope related to this item is addressed in the Master Policy.

5.1.6. Storage media

The scope related to this item is addressed in the Master Policy.

5.1.7. Destruction of redundant media and information

The scope related to this item is addressed in the Master Policy.

5.1.8. Backup storage

The scope related to this item is addressed in the Master Policy.

5.1.9. Registration points security controls

The scope related to this item is addressed in the Master Policy.

5.1.9.1. Site location and facility

The scope related to this item is addressed in the Master Policy.

5.1.9.2. Physical access

The scope related to this item is addressed in the Master Policy.

5.1.9.3. Power and air conditioning

The scope related to this item is addressed in the Master Policy.

5.1.9.4. Water hazard

The scope related to this item is addressed in the Master Policy.

5.1.9.5. Fire prevention and protection

The scope related to this item is addressed in the Master Policy.

5.1.9.6. Storage media

The scope related to this item is addressed in the Master Policy.

5.1.9.7. Destruction of information

The scope related to this item is addressed in the Master Policy.

5.1.9.8. Backup storage

The scope related to this item is addressed in the Master Policy.

5.1.10. Service recipient security

The recipient should protect his/her password to access the system and personal identification number (PIN). If the password or PIN used is difficult to remember, it may be saved, however, provided that it is stored in a safe, to which only the service recipient has access, or that the password is encrypted (with an algorithm known to the owner of the PIN in question).

5.2. Organizational security controls

The scope related to this item is addressed in the Master Policy.

The following is a list of roles that employees of Certum may perform and is consistent with the requirements described in *ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers* and *ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.*

5.2.1. Trusted roles

5.2.1.1. Trusted roles in Certum

The scope related to this item is addressed in the Master Policy.

Certum identifies the trusted roles described in the Master Policy and the Identity Verification Inspector:

- **Identity Verification Inspector** – responsible for verifying the identity of customers (sender and addressee) following a defined initial identity verification process in accordance with *ETSI 319 521*.

The role of the Identity Verification Inspector is performed by the Registration Inspector, who also exercises all the functions of the former.

Individual roles and responsibilities related to them are documented in Certum's internal procedures, moreover, responsibilities are described in individual contracts with employees (including temporary employees).

5.2.1.2. Trusted roles in the registration system point

Certum has to be sure that the personnel of the registration system point understands their responsibility, arising from the necessity of credible identification and authentication of the customer. Due to above, the following roles are distinguished in the registration system point:

- **person who verifies identity of the applicant** – verifies the customer's identity and the correctness of the application submitted by him/her and accepts the terms of the eDelivery service on behalf of Asseco Data Systems S.A.,

- **partner establishing the authorized registration point –** is responsible for efficient operation of the registration system point; **its role is to provide funding for staff, manage the work of people who confirm the identity of customers.**

A person who verifies identity of customers must be accredited by Certum. After obtaining it (at his/her own request or at the request of a Partner of the authorized registration point), he/she can verify the identity of customers both at the registered office of the registration point and at the place of residence of the customer.

5.2.1.3. Customer's trusted roles

This eDelivery Policy does not specify any requirements in this regard.

5.2.2. Number of persons required per task

The scope related to this item is addressed in the Master Policy.

5.2.3. Identification and authentication for each role

The scope related to this item is addressed in the Master Policy.

5.2.4. Roles that cannot be combined

The scope related to this item is addressed in the Master Policy.

5.3. Personnel controls

The scope related to this item is addressed in the Master Policy.

5.3.1. Qualifications, experience and authorization

The scope related to this item is addressed in the Master Policy.

5.3.2. Personnel verification procedure

The scope related to this item is addressed in the Master Policy.

5.3.3. Training requirements

The scope related to this item is addressed in the Master Policy.

Personnel performing activities under the eDelivery service must be trained in the procedure for verifying the identity of customers and operating the system.

5.3.4. Retraining Frequency and Requirements

The scope related to this item is addressed in the Master Policy.

5.3.5. Job rotation

The scope related to this item is addressed in the Master Policy.

5.3.6. Sanctions for unauthorized actions

The scope related to this item is addressed in the Master Policy.

5.3.7. Contract personnel

The scope related to this item is addressed in the Master Policy.

5.3.8. Documentation supplied to personnel

The scope related to this item is addressed in the Master Policy.

5.4. Events recording, security incidents management and security audits

The scope related to this item is addressed in the Master Policy.

5.4.1. Types of events recorded

The scope related to this item is addressed in the Master Policy.

5.4.2. Frequency of events logs checking

The scope related to this item is addressed in the Master Policy.

5.4.3. Event logs retention period

The scope related to this item is addressed in the Master Policy.

5.4.4. Protection of event logs

The scope related to this item is addressed in the Master Policy.

5.4.5. Procedures for event logs backups

The scope related to this item is addressed in the Master Policy.

5.4.6. Collecting data for internal and external audit

The scope related to this item is addressed in the Master Policy.

5.4.7. Notifying entities responsible for the event

The scope related to this item is addressed in the Master Policy.

5.4.8. Vulnerability assessment

The scope related to this item is addressed in the Master Policy.

5.5. Data archiving

It is required that all data and files pertaining to recorded system security data, applications submitted by customers, information about customers, evidence of events occurring within the delivery process are archived.

Archival copies of electronic data are retained at the **main and alternate** Certum site**.**

5.5.1. Types of data archived

The following data is archived:

- data confirming the identity of the customer (sender and addressee),
- documents issued by the registration system point operator, confirming the identity of customers on behalf of Certum,
- the terms of the eDelivery service accepted by the customer,
- database of customers, including all information collected during the customer registration process,
- other documents and data related to the provision of the eDelivery service.

The following service-related evidence is also archived:

- events that occur during the transfer of data between parties,
- evidence from a service that a specific event related to the process of transmitting specific data between the sender and the addressee occurred at a specific time,

- time stamp tokens corresponding to the date and time the message was sent as well as transmitted and modified, as appropriate.

5.5.2. Archive retention period

Archived data (in electronic form), listed in chapter 5.5.1 are retained for the period of 20 years. After expiration of the accepted archiving period, the data is destroyed.

Events related to the submission, transmission and transfer of a message is retained for at least 36 months depending on the business package purchased.

5.5.3. Archive protection

The scope related to this item is addressed in the Master Policy.

5.5.4. Backup procedures

The scope related to this item is addressed in the Master Policy.

Backup copies allow full restoration (if necessary, e.g. after a system failure) of data necessary for the normal operation of the service.

Backup copies are created by Certum personnel in trusted roles. Backup copies are subject to periodic verification, restoration according to Certum's internal procedures.

To prevent data loss, the eDelivery service guarantees data protection using backup and data replication mechanisms at least once every 24 hours. This means that data recovery in the event of software or infrastructure failure is carried out in accordance with the following indicators:

- RPO (Recovery Point Objective) for the service is 24 hours.
- RTO (Recovery Time Objective) for the service is 24 hours.

5.5.5. Requirements for electronic time-stamping of the data archived

The scope related to this item is addressed in the Master Policy.

5.5.6. Archival data collection system (internal and external)

The scope related to this item is addressed in the Master Policy.

5.5.7. Procedures to obtain and verify archived information

The scope related to this item is addressed in the Master Policy.

5.6. Key changeover

The key changeover procedure refers to the eDelivery service key and concerns procedure for key update (rekey) which replaces the key currently used to sign proofs of service.

Rekey procedure for the mentioned above eDelivery service consists in applying to the National Certification Authority for a new trust service provider certificate. Upon receipt of the certificate, that authority issues to National certification authority a mutual certificates of trust service providers.

Each eDelivery service key changeover is announced in advance by means of Certum repository.

5.7. Key security violation and disaster recovery

The scope related to this item is addressed in the Master Policy.

5.7.1. Procedures for handling incidents and respond to threats

The scope related to this item is addressed in the Master Policy.

5.7.2. Corruption of computing resources, software and/or data

The scope related to this item is addressed in the Master Policy.

5.7.3. Certification authority private key compromise or suspected compromise

The scope related to this item is addressed in the Master Policy.

5.7.4. Business continuity capabilities after a disaster

The scope related to this item is addressed in the Master Policy.

5.8. Termination of activity or delegation of tasks by the eDelivery service

The obligations of the eDelivery service presented below aim at reducing the impact of Certum's decision to terminate its activity and include the obligation to inform in due time the supervisory body, customers, contractors, and Partners with whom the Center is bound by commercial agreements about this fact and to transfer documents and data related to the provision of the service to the supervisory body. The Center's termination plan, which is Certum's internal procedure, sets out the detailed procedure to be followed in the event of termination of the Center's operations.

The Supervisory Authority shall be informed of plans to terminate Certum's operations, and of any significant change thereto.

5.8.1. Requirements associated with duty transition

In case of terminating its operations, Certum shall be obliged to:

- notify **the National Certification Center** of its intention to cease operations as a qualified provider of the eDelivery service; at least 90 days before the planned termination of its operations,
- notify (at least 90 days in advance) all customers of the intent to terminate operations,
- notify the Trading Partners and Partners operating Identity Confirmation Points and notify the Registration Points,
- notify other entities with which Certum is bound by commercial agreements for the provision of eDelivery services,
- inform all customers associated with the eDelivery service of the termination of operations,
- cancel all powers of attorney to confirm the identity of customers and to sign eDelivery service agreements on behalf of Asseco Data Systems S.A.,
- transfer data directly related to the performance of the eDelivery service to the Supervisory Authority or to the entity designated by it, including the eDelivery service keys, customer registration documents, event logging, and all information that is necessary to provide evidence of messages, including the obligation to ensure their availability for an appropriate period of time (for a period of 20 years from their creation),
- conclude agreements necessary for the proper transfer of the data and the service (referred to above) with the entities taking them over, containing an obligation to retain them for the period indicated by law, i.e.: for 20 years from their creation,
- destroy the eDelivery service keys and their backups when no further use is anticipated or when the eDelivery service provider certificate associated with the service is revoked,
- reimburse to the customer or an entity represented by the customer of the costs, in proportion to the remaining term of the service.

5.8.2. Proceedings in case of termination of operations

Certum's termination plan, which is Certum's internal procedure, shall set forth in detail how Certum shall proceed in the event of termination.

All currently valid certificates of the eDelivery service provider must be revoked on the date of declared definitive termination of operations and placed on the CRL. Private keys of the eDelivery service must be destroyed.

6. Technical safety controls

This chapter describes the procedures for the generation and management of Certum cryptographic key pairs, along with the associated technical requirements.

6.1. Key pair generation and installation

6.1.1. Key pair generation

Procedures for the key management address the secure storage and usage of keys under Certum's control, influencing secure operation of the entire service.

The private key of the eDelivery authority is generated and secured at the same level as the keys of other authorities in accordance with the Master Policy.

The eDelivery service has at least one certificate of the Certum QERDS 2023 trust service provider, which is used in the qualified electronic registered delivery process.

6.1.1.1. Public and private key generation

The scope related to this item is addressed in the Master Policy.

6.1.1.1.1 Procedures for generating initial keys of the certification authority

The scope related to this item is addressed in the Master Policy.

6.1.1.1.2 Certification authority keys re-key procedures

The scope related to this item is addressed in the Master Policy.

Certum QERDS 2023 authority keys have a finite lifetime, before which they must be updated.

The Certum QERDS 2023 Authority remains valid as long as the algorithms used to create it remain considered secure.

The maximum time after which a Certum QERDS 2023 Authority certificate will need to be renewed based on the new algorithms is determined in accordance with ETSI TS 119 312 (Recommended key sizes versus time).

6.1.2. Private key delivery to end user

Not applicable.

6.1.3. Public key delivery to a certification authority

The transfer takes place in accordance with the rules of the National Certification Center described in the Certification Policy of the National Certification Center.

6.1.4. Certification authority public key delivery to relying parties

The scope related to this item is addressed in the Master Policy.

6.1.5. Keys sizes

The scope related to this item is addressed in the Master Policy.

6.1.6. Public key generation parameters and quality checking

The scope related to this item is addressed in the Master Policy.

6.1.7. Key usage purposes

The scope related to this item is addressed in the Master Policy.

6.1.8. Hardware and/or software key generation

The scope related to this item is addressed in the Master Policy.

Also applies to the eDelivery service.

6.2. Private key protection

The scope related to this item is addressed in the Master Policy.

6.2.1. Standards for cryptographic modules

The scope related to this item is addressed in the Master Policy.

The hardware cryptographic modules used by the eDelivery service shall comply with the requirements of FIPS 140, Common Criteria EAL 4+.

Tab. 1 Minimal requirements imposed on hardware security modules

Certificate subject type	Employed security module
Certification authority Certum QERDS 2023	Hardware, complying with FIPS 140-2 Level 3 or higher / EAL 4+

6.2.2. Private key multi-person control

The scope related to this item is addressed in the Master Policy.

Shared secrets are stored on smart cards, protected by a PIN number and transferred in a secure manner to the holders of the shared secret.

Division and distribution of shared secrets of the eDelivery service

Name of the trust service provider	Number of shared secrets required for private key restoration	Total number of secrets distributed
Certum QERDS 2023	3	5

Shared secret transfer procedure has to include secret holder presence during key generation and distribution process, acceptance of a delivered secret and resulting responsibility for its storage, and it should state conditions and requirements for shared secret retransmission to authorized personnel.

6.2.2.1. Acceptance of a secret shared by its holder

The scope related to this item is addressed in the Master Policy.

6.2.2.2. Protection of a shared secret

The scope related to this item is addressed in the Master Policy.

6.2.2.3. Availability and erasure (transfer) of a shared secret

The scope related to this item is addressed in the Master Policy.

6.2.2.4. Responsibilities of shared secret holder

The scope related to this item is addressed in the Master Policy.

6.2.3. Private key escrow

The scope related to this item is addressed in the Master Policy.

6.2.4. Private key backup

The scope related to this item is addressed in the Master Policy.

6.2.5. Private key archiving

The scope related to this item is addressed in the Master Policy.

Also applies to the private key of the eDelivery service.

6.2.6. Private key entry into cryptographic module

The scope related to this item is addressed in the Master Policy.

Also applies to the private key of the eDelivery service.

6.2.7. Private key storage in cryptographic modules

The scope related to this item is addressed in the Master Policy.

6.2.8. Method of activating private key

The scope related to this item is addressed in the Master Policy.

These rules apply also to the private key of the eDelivery service.

6.2.9. Method of deactivating private key

The scope related to this item is addressed in the Master Policy.

These rules apply also to the private key of the eDelivery service.

6.2.10. Method of destroying private key

The scope related to this item is addressed in the Master Policy.

These rules apply also to the private key of the eDelivery service.

6.2.11. Cryptographic modules rating

The scope related to this item is addressed in the Master Policy.

6.3. Other aspects of key management

The scope related to this item is addressed in the Master Policy.

6.3.1. Public key archiving

The scope related to this item is addressed in the Master Policy.

6.3.2. Usage periods of public and private keys

The scope related to this item is addressed in the Master Policy.

Standard maximum validity periods for private keys and associated certificates of the eDelivery Authority trust service provider.

Owner and key type		Main key usage	
		RSA for certificate and CRL signing	RSA for token signing
Certum QERDS 2023	supplier certificate	–	11 years
	private key	–	11 years

6.4. Activation data

The scope related to this item is addressed in the Master Policy.

These rules also apply to the eDelivery service.

6.4.1. Activation data generation and installation

The scope related to this item is addressed in the Master Policy.

6.4.2. Activation data protection

The scope related to this item is addressed in the Master Policy.

6.4.3. Other aspects of activation data

The scope related to this item is addressed in the Master Policy.

6.5. Computer security controls

The scope related to this item is addressed in the Master Policy.

These rules also apply to the eDelivery service.

6.5.1. Specific computer system security technical requirements

The scope related to this item is addressed in the Master Policy.

6.5.2. Computer security rating

The scope related to this item is addressed in the Master Policy.

6.6. Technical control

The scope related to this item is addressed in the Master Policy.

These rules also apply to the eDelivery service.

6.6.1. System development controls

The scope related to this item is addressed in the Master Policy.

6.6.2. Security management controls

The scope related to this item is addressed in the Master Policy.

6.6.3. Life cycle security ratings

The scope related to this item is addressed in the Master Policy.

6.7. Network security controls

The scope related to this item is addressed in the Master Policy.

6.8. Time-stamping

All messages within the eDelivery service are time-stamped with the date and time of sending, receipt, and any change by a qualified electronic time stamp.

The electronic time stamps created within the Certum system for the above-mentioned purposes are in accordance with ETSI EN 319 422 (see chapter 1.3.1.2**Błąd! Nie można odnaleźć źródła odwołania.** of the Master Policy).

7. Certificate profiles

7.1. Profile of eDelivery Service

The eDelivery service issues electronic proofs signed with the Certum QERDS 2023 certificate of authority. The proof contains information that at a certain point in time a specific event took place related to the data transmission process between the sender and the addressee (e.g. sending or receiving a message).

Service identifiers included in the confirmations issued by Certum eDelivery:

Confirmation Name	Service identifier
Confirmation of receipt	1.2.616.1.113527.2.4.1.4.2
Confirmation of submission	1.2.616.1.113527.2.4.1.4.4

7.2. Other profiles

7.2.1. Electronic time stamp token profile

The scope related to this item is addressed in the Master Policy.

7.2.2. Validation token profile for electronic signatures and electronic seals

The scope related to this item is addressed in the Master Policy.

7.2.3. Certificate status verification token profiles

The scope related to this item is addressed in the Master Policy.

8. Compliance audit and other evaluations

The purpose of the audit is to determine the extent to which the conduct of Certum's service unit or its designated elements complies with the Integrated Quality and Information Security Management System implemented by Asseco Data Systems S.A. Integrated Quality and Information Security Management System, which includes in particular the requirements of PN-EN ISO 9001 and PN-ISO/IEC 27001 standards, as well as Certum's internal declarations and procedures.

Audits of Certum's compliance of its conduct with the requirements imposed on eDelivery service providers set forth in the eIDAS Regulation, the requirements of the RDE service standard, and the procedures and processes described in Certum's internal documentation (including verification of trusted roles defined in Certum).

Certum audit may be conducted by internal units of Asseco Data Systems S.A. (**internal audit**) and by organizational units independent of Asseco Data Systems S.A. (**external audit**).

8.1. Audit frequency and circumstances

The scope related to this item is addressed in the Master Policy.

8.2. Identity/qualifications of the Auditor

The scope related to this item is addressed in the Master Policy.

8.3. Auditor relationship with audited entity

The scope related to this item is addressed in the Master Policy.

8.4. Topics covered by the audit

The scope related to this item is addressed in the Master Policy.

8.5. Actions taken to address discrepancies identified during the audit

The scope related to this item is addressed in the Master Policy.

8.6. Notifying of audit results

The certificate of compliance of the eDelivery service received is published on the website available at www.certum.pl.

9. Other business and legal matters

9.1. Fees

Certum charges fees for its services. The amounts of fees and the types of services covered by the fees are published in the price list, available in the Certum Certification Authority repository **on** the website:

www.certum.pl

9.1.1. Fees for other services

The scope related to this item is addressed in the Master Policy, item 9.1.4.

9.1.2. Fees refund

Certum is committed to providing the highest level of service. In any other case, the Customer may demand a refund of the fee paid if the eDelivery service was not performed in accordance with the rules resulting from the terms of trust services and the provisions hereof.

Fees refund claims should be submitted to the addresses stated in chapter 1.5.2.

9.2. Financial responsibility

Responsibility of Asseco Data Systems S.A. through its business unit operating under the name of Certum as well as of the parties affiliated through services provided by that unit arises out of routine activities performed by those entities or actions of third parties. The responsibility of each entity is defined in mutual agreements or arises from statements of will.

Certum is responsible for existence of the situations listed in chapter 9.9 of this document.

Certum is financially responsible to the customers of the eDelivery service who rely on its operations.

Certum's financial responsibility shall apply only if the damage occurs due to Certum's fault or due to the fault of parties with whom Asseco Data Systems S.A. has agreements stating that the fault is transferred to Certum.

Certum shall not bear financial responsibility as defined herein to other third parties who are not customers of the eDelivery service.

In the event of a damage, the customer must report the damage within 30 days of its occurrence. If a damage is reported at a later date, Certum is not obliged to process the damage in question.

Certum shall bear financially responsibility only during the period of indemnification depending on the business package purchased.

If Certum's employees confirm the occurrence of damage, Asseco Data Systems S.A. undertakes to pay compensation. The amount of compensation for a single loss cannot exceed the financial guarantee limit for a single loss. The amount of compensation paid will not be more than the proven value of the damage.

Asseco Data Systems S.A. shall pay out compensation for the reported damages in the order of their occurrence.

9.2.1. Insurance coverage

The scope related to this item is addressed in the Master Policy.

9.2.2. Other assets

The scope related to this item is addressed in the Master Policy.

9.2.3. Extended warranty coverage

The scope related to this item is addressed in the Master Policy.

9.3. Confidentiality of business information

The scope related to this item is addressed in the Master Policy.

9.3.1. Types of information to be kept secret

The scope related to this item is addressed in the Master Policy.

9.3.2. Types of information not considered confidential

The scope related to this item is addressed in the Master Policy.

Moreover, all information which is necessary in the process of proper functioning of the eDelivery service shall be considered as non-confidential information.

In addition, the documents listed below are treated as publicly available through the Certum website available at www.certum.pl:

- Terms & Conditions of Certum eDelivery Qualified Trust Service – electronic registered delivery

- Policy and Practice Statement of Certum eDelivery Qualified Service – electronic registered delivery

9.3.3. Obligation to protect confidentiality of information

The scope related to this item is addressed in the Master Policy.

9.4. Privacy of personal information

9.4.1. Privacy Policy

The scope related to this item is addressed in the Master Policy.

9.4.2. Information considered as private

Any information about the customer that is not necessary for the proper functioning of the eDelivery service.

9.4.3. Information not considered as private

All information made publicly available shall not be considered as private information, as long as this rule does not violate the requirements under *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 and repealing Directive 95/46/EC*.

9.4.4. Responsibility to protect private information

The scope related to this item is addressed in the Master Policy.

9.4.5. Reservations and permission to use private information

The scope related to this item is addressed in the Master Policy.

9.4.6. Sharing information in accordance with a court or administrative order

The scope related to this item is addressed in the Master Policy.

9.4.7. Other disclosure circumstances

The scope related to this item is addressed in the Master Policy.

9.5. Intellectual property rights

The scope related to this item is addressed in the Master Policy.

9.5.1. Trademark

The scope related to this item is addressed in the Master Policy.

9.6. Commitments and guarantees

This chapter outlines the obligations and responsibilities of Certum, the registration points (including identity confirmation points), the users of the eDelivery service (customers and relying parties). These obligations and liabilities are governed by mutual agreements between the parties.

The subject of the agreement concluded between Asseco Data Systems S.A. and the customer is the qualified eDelivery service made available by Certum, mutual obligations and liabilities, including financial ones. The detailed description can be found in the Terms & Conditions of Certum eDelivery Qualified Trust Service – electronic registered delivery

9.6.1. Commitments and guarantees of the eDelivery service

Providing the qualified eDelivery service, Certum guarantees that:

- it follows and enforces the procedures described in this document,
- it uses devices and technologies that ensure system reliability and technical and cryptographic security in process execution,
- provision of the eDelivery service after verification of the information provided by means permitted by law,
- any change of data required to send or receive the data is clearly indicated to the sender and addressee of the data,
- it provides accurate time stamping for sending and receiving messages – electronic time stamping services,
- the availability, integrity and confidentiality of user's content is guaranteed from the time it is sent to the time it is received,
- the integrity of user content is protected, particularly in sender/addressee exchanges,
- evidence of posting is issued after the message is posted without waiting for return status,
- evidence related to user content delivery activities is protected by a qualified electronic seal that precludes alteration of data,
- Each electronic delivery address is assigned one box with guaranteed capacity,
- the size of a single message cannot exceed 15 MB,
- the service allows you to attach a maximum of 25 attachments at the same time (including the content of the message),
- Overfilling of the recipient's delivery box will result in the inability to send and receive correspondence until the recipient releases the capacity in the delivery box,
- in cases where modification of user content is required, these modifications are clearly indicated to the sender, addressee and possible third parties,
- it ensures immediate action is taken in the event of technical security issues,
- ensures delivery time according to the RDE service standard,
- guarantees data protection using backup and data replication mechanisms at least once every 24 hours,
- continuous access to the services is provided, 24/7/365 excluding the following interruptions:
  - scheduled and pre-announced technology repairs related to equipment and system maintenance;
  - unplanned technological repairs to infrastructure as a result of unforeseen failures;
  - maintenance caused by infrastructure failures outside Certum's jurisdiction;
  - unavailability of the service as a result of Force Majeure or extraordinary events.
- it will give notice of maintenance or upgrade of its infrastructure at least three days before the start of the repair
- it protects personal data of customers in accordance with *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 and repealing Directive 95/46/EC* and its implementing documents,
- it employs staff with knowledge, qualifications and experience appropriate to perform functions related to the eDelivery service, including but not limited to the areas of:

  - automatic data processing in data communication networks and systems,
  - mechanisms for securing ICT networks and systems,
  - cryptography, electronic signatures and seals, and public key infrastructure,
  - hardware and software used for electronic data processing,

Certum further undertakes to:

- keep confidential any information related to the provided eDelivery services, unauthorized disclosure of which might put Asseco Data Systems S.A. or the recipient of trust services at risk, for the period of 10 years following the termination of legal relations referred to in Article 15(3) of the *Act*, and to keep indefinitely confidential the data used for the submission of electronic certificates, as well as to
  a. retain for 20 years all information about customers of the eDelivery service collected during the identity verification process,
  b. retain for 20 years all authentications issued by the eDelivery service,
  c. retain for at least 36 months (RDE service standard item 5.1.12.9) all event records it has created in a manner that allows them to be viewed electronically.

All clocks operating within the Certum system providing qualified services and used in the course of providing services are synchronized to the Coordinated Universal Time (UTC), with the accuracy of 1 second.

Certum does not provide the eDelivery service to minors (under 18 years of age), even if they run a business.

9.6.1.1. Certification authority repository obligations

The scope related to this item is addressed in the Master Policy.

9.6.2. Registration Points obligations and guarantees

The scope related to this item is addressed in the Master Policy.

9.6.3. Customer obligations and guarantees

By submitting an application for access to the eDelivery service and accepting the terms of the service, the customer agrees to join the service under the terms of the eDelivery service, the Master Policy, the eDelivery Policy and the Terms & Conditions of eDelivery Qualified Trust Service.

The Customer is obliged to:

- comply with the terms of the eDelivery service provided by Asseco Data Systems S.A.,
- provide the serving point of the Registration System network with true and correct information at each stage of cooperation,
- provide documents verifying the accuracy of the data contained in the application in order to fulfill the requirements of the registration process as set forth in the Master Policy/eDelivery Policy,
- inform Certum immediately of any errors or changes in data,
- use the eDelivery service only for lawful purposes,
- is obliged to send files free from viruses and malware.

The service recipient is liable for damage resulting from sending infected parcels.

The Customer is responsible for the correctness of the entries in his/her address book (contacts). The entries in the customer's address book are not subject to Certum's supervision. The customer is the controller of the personal data kept in his/her address book (contacts).

The service recipient, i.e. the owner of the eDelivery services, supervises and allows access to the eDelivery services to other users on his own. Such users are not subject to Certum's supervision. The Service Recipient is the administrator of the personal data of other users that it maintains in its eDelivery services.

9.6.4. Relying parties commitments and guarantees

Depending on mutual relations between the relying party and Certum or the customer, the obligations of the relying party may be expressed in the form of an agreement with Asseco Data Systems S.A. or the customer or may have the character of acceptance of the terms of trust services.

Regardless of the nature of the agreement, the relying party is obliged to:

- thoroughly verify each confirmation received by it. For that purpose, the relying party shall:
  - verify that all certificates of trust service providers included in the certification path belong to certification authorities and that they have been granted the right to certify electronic registered deliveries,
  - specify the date and time of confirmation. This is done with a qualified electronic time stamp embedded in the confirmation.

If a document or electronic signature is time-stamped or in any way associated with other tokens or confirmations issued by Certum, then in order to reasonably establish trust in the verified token or confirmation, the relying party should additionally:

- verify whether the token or confirmation was properly electronically verified and whether the private key used by the Certum QTST 2017 qualified electronic time stamp authority was not disclosed until the token or confirmation was verified (unless the time contained therein meets the date certain requirements); the status of the private key can be verified based on the verification of the corresponding public key,
- check the restrictions on the use of the service in this eDelivery Policy document and Certum's terms of trust services.

9.6.5. Other users commitments and guarantees

This eDelivery Policy does not specify any requirements in this regard.

9.7. Warranty disclaimer

Certum guarantees are based on the general principles of this eDelivery Policy and comply with the statutory legal acts currently in force in the Republic of Poland. Certum warranty disclaimer is included in in the terms of trust services by Certum.

9.8. Liability

Certum**, acting** within the authorization of Asseco Data Systems S.A., shall be liable for the effects of operation of the **eDelivery** service, the Primary Registration Point and other points of the registration system as well as persons confirming identity to the extent specified in the terms of the eDelivery service.

Certum's activities are supported by other departments of Asseco Data Systems S.A. on the basis of specialized internal outsourcing.

The liability provisions of the parties set forth below do not eliminate or replace liability under separate provisions of law.

9.8.1. Certum liability

9.8.1.1. eDelivery service liability

The eDelivery service shall be liable in cases where direct and indirect damages incurred by the user:

- have arisen despite the user's compliance with the eDelivery Policy and the Master Policy,
- are the result of proven mistakes made by the **eDelivery service**,
- have occurred as a result of the violation of other Certum warranties set forth in 9.6.1.

Certum outsources the services of running the so-called Identity Confirmation Points to external entities. Despite the fact that the registration point is contractually bound to Asseco Data Systems S.A., Certum bears full responsibility for the part of its work that is related to the provision of trust services by Certum.

Certum shall not be liable for any failure or unreliability of the services on the part of the Partner.

Certum does not outsource any services other than registration services.

Certum shall not be liable for the unavailability of the service due to the unavailability of the EAD and the DO – designated operator.

At the same time, Certum shall not be liable for the actions of third parties, customers or other parties not affiliated with Certum. In particular, Certum shall not be liable:

- for damage caused by Force Majeure or other circumstances for which it is not responsible, i.e.: fire, flood, windstorm, war, acts of terror, epidemics and other natural or man-made disasters,
- for damages resulting from the installation, use and management of applications other than those provided by Certum,
- in the event the customer provides false data and, despite Certum's due diligence, such data is entered, upon the request of the customer, both in Certum's databases as well as in the eDelivery service.

9.8.1.2. Certification authority liability

The scope related to this item is addressed in the Master Policy.

9.8.1.3. Customer liability

The customer's liability is based on the obligations and limitations set forth in chapter 9.6.3 of this document.

9.8.1.4. Relying party liability

The relying party's liability is based on the obligations and warranties set forth in chapter 9.6.4.

The terms and conditions of such liability may also be governed by an agreement concluded with the customer and Asseco Data Systems S.A. or acceptance of the terms of the eDelivery service.

9.9. Compensations

9.9.1. Customer civil liability compensation

Customers' civil liability compensation is based on the obligations and warranties set forth in chapter 9.6.3 of this document.

9.9.2. Relying party civil liability compensation

Relying parties' civil liability compensation is based on the obligations and warranties set forth in chapter 9.6.4 of this document.

9.10. Policy and Practice Statement of eDelivery Qualified Service validity period

9.10.1. Validity period

This Policy and Practice Statement of Qualified eDelivery Service is in effect from the moment of changing its status to valid and publication in Certum's repository until the publication of the next valid version.

9.10.2. Expiration

This document is valid until it is replaced with a new version. The starting date of the validity of the new version of the Policy and Practice Statement of eDelivery Qualified Service is also the expiry date of this Policy.

9.10.3. The policy and Practice Statement of eDelivery Qualified Service expiry effects and transition period

Upon expiration of the previous version of the document, users of the eDelivery service are obliged to comply with the provisions of this document until it expires.

9.11. Users notification and communication

The scope related to this item is addressed in the Master Policy.

9.12. Amendment procedure

The scope related to this item is addressed in the Master Policy.

9.12.1. Revision procedure

The scope related to this item is addressed in the Master Policy.

9.12.1.1. Amendments that do not require notification

The scope related to this item is addressed in the Master Policy.

9.12.2. Notification mechanism and comment period

The scope related to this item is addressed in the Master Policy.

9.12.2.1. Comment period

The scope related to this item is addressed in the Master Policy.

9.12.3. Changes requiring new identifier

The scope related to this item is addressed in the Master Policy.

9.12.4. Publication of a new version of the Policy and Practice Statement of eDelivery Qualified Service and Terms & Conditions of Qualified Trust Services

The scope related to this item is addressed in the Master Policy.

Also applies to the eDelivery service.

9.12.5. Items not published in the Policy and Practice Statement of eDelivery Qualified Service

The scope related to this item is addressed in the Master Policy.

Also applies to the eDelivery service.

9.13. Dispute resolution, complaints

The subject of disputes resolution, including complaints, can only be discrepancies or conflicts between the parties in respect to the eDelivery service based on the provisions of the eDelivery Policy, the Master Policy and agreements concluded.

Disputes, complaints or grievances arising out of the use of the service will be resolved based on written information through mediation. Complaints should be addressed in writing to:

Asseco Data Systems S.A.
Królowej Korony Polskiej 21 Street
70-486 Szczecin, Poland

Disputes related to the eDelivery Service will be resolved through conciliation in the first instance.

Complaints shall be resolved in writing within 21 days of delivery to the above address. If the dispute is not resolved within 45 days of the commencement of conciliation, the parties shall be entitled to take court action. The Common Court of venue for the defendant will have jurisdiction to hear the case.

Should other disputes arise out of the use of the service provided by Certum, the customer undertakes to inform Certum in writing of the subject matter of the dispute arising.

9.14. Governing law

9.14.1. Survival of provisions

The scope related to this item is addressed in the Master Policy.

Also applies to the eDelivery service.

9.14.2. Provision references

The scope related to this item is addressed in the Master Policy.

Also applies to the eDelivery service.

9.15. Compliance with applicable law

Certum functioning is based on the principles contained in this eDelivery Policy and law applicable in the territory of Poland.

9.16. Other laws

The present eDelivery Policy and the Master Policy do not specify any conditions in this regard.

9.16.1. Completeness of contractual terms

The present eDelivery Policy and the Master Policy do not specify any conditions in this regard.

9.16.2. Assignment of rights

The present eDelivery Policy and the Master Policy do not specify any conditions in this regard.

9.16.3. Severability

The scope related to this item is addressed in the Master Policy.

9.16.4. Enforcement clause

The scope related to this item is addressed in the Master Policy.

9.16.5. Force Majeure

The scope related to this item is addressed in the Master Policy.

9.17. Other provisions

The present eDelivery Policy and the Master Policy do not specify any conditions in this regard.

10. Documentary history

Document revision history		
1.0	November 15th, 2022	Development of the document.
1.1	February 26th, 2024	Adding information on the frequency of backup copies, the maximum number of attachments and the possibility of confirming identity based on mDowód document and Polish residence card.

Appendix 1: Glossary

Addressee – the entity specified by the sender as the recipient of the message.

API (Application Programming Interface) - an application programming interface, i.e. a defined set of rules that allows access to a service.

Certificate Policy – The "Policy and Practice Statement of Certum eDelivery Qualified Service – electronic registered delivery" is a set of rules defining in particular the principles of provision of trust services, liability of the parties, available in an electronic form at www.certum.pl.

Certum – an organizational unit of Asseco Data Systems S.A. entered in the register of qualified trust service providers maintained by the National Bank of Poland on behalf of the minister responsible for information technology. This registry is published at the web address: www.nccert.pl.

Customer – a natural person applying for access to the service and for whom access has been granted.

BAE – a database of electronic addresses, which is a public registry where addresses for electronic delivery are collected, maintained by the minister responsible for information technology.

eDelivery box - a tool enabling sending, receiving and storing data as part of the eDelivery service.

eDelivery Qualified Service – electronic registered delivery – provided by Certum QERDS 2023. Means a service that enables data to be sent between third parties electronically and provides evidence associated with the handling of the data sent, including proof of sending and receiving the data, and protects the data sent from the risk of loss, theft, damage or any unauthorized alteration.

Electronic delivery address (ADE)– electronic address, referred to in Art. 2 (1) of the Polish Act of 18 July 2002 on provision of services by electronic means, of the entity using the public electronic registered delivery service or the public hybrid service or the qualified electronic registered delivery service, allowing for the unambiguous identification of the sender or addressee of the data sent under those services.

Address for electronic deliveries created by the minister responsible for digitization, in a way that ensures its uniqueness and precise assignment to a public entity, non-public entity, including a natural person.

EU 910/2014 eIDAS Regulation – Regulation No. 910/2014 of the European Parliament and of the Council (EU) of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC. The regulation is a legal act binding in its entirety in the Polish legal system and in all countries of the European Union.

Identification data – data that unambiguously identifies the customer and whose accuracy can be confirmed on the basis of the customer's identity document.

Polish Act on Trust Services and Electronic Identification – the Act of 5 September 2016 on Trust Services and Electronic Identification (OJ of 2021, item 1797, as amended died).

Polish Electronic Delivery Act – of 18 November 2020 on electronic delivery (Journal of Laws 2020, item 2320).

Polish Regulation on guaranteed availability and capacity of delivery boxes for public and non-public entities using the public registered electronic delivery service – of 24 June 2021 (Journal of Laws 2021, item 1202).

Registration system point - Identity Confirmation Point (PPT) and Registration Point (PR) - its function is to confirm the identity of service recipients and accept the terms of providing trust services in the process of applying for access to the selected service.

Sender – a natural or legal person delivering the contents of the message.