Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service - certificate issued in the signing process

Version 1.2

Effective date: October 27th 2023 r.

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

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

Trademark and Copyright notices

Content

1. Introduction 11
1.1. Overview 12
1.2. Document Name and its Identification 12
1.3. CISP Policy Parties 12
1.3.1. Trust Services Authorities 13
1.3.2. Primary Registration Authority, Registration authorities and points of the identity verification 13
1.3.3. Subscribers 13
1.3.4. Relying Parties 13
1.3.5. Other Parties 13
1.4. Certificate and certificate of trust service provider usage 13
1.4.2. Prohibited Certificate Uses 14
1.5. Certificate Policy and Certification Practice Statement Administration 14
1.5.1. Organization responsible for administrating the document 14
1.5.2. Contact 14
1.5.3. Entities determining the validity of the principles contained in the document 14
1.5.4. Approval Procedures 15
1.6. Definitions and abbreviations 15
2. Publication and Repository 15
2.1. Repository 15
2.2. Information Published by Certum 15
2.3. Frequency of Publication 15
2.4. Access to Publications 15
3. Identification and Authentication 15
3.1. Naming 15
3.1.1. Types of Names 15
3.1.2. Need for Names to be Meaningful 15
3.1.3. Subscribers anonymity 16
3.1.4. Rules for Interpreting Various Names Forms 16
3.1.5. Names Uniqueness 16
3.1.6. Recognition, Authentication and Role of Trademarks 16
3.2. Initial Registration 16
3.2.1. Proof of Possession of Private Key 16
3.2.2. Authentication of the subscriber's rights and other attributes 16
3.2.3. Authentication of natural person's identity 16
3.2.4. Non-Verified Subscriber Information 17

3.2.5. Validation of Authority 17
3.2.6. Interoperability criteria 17
3.3. Subscriber's Identity Authentication for Certificate Rekey or Certificate Data Modification requests 18
3.3.1. Identification and authentication in a standard rekey 18
3.3.2. Authentication for issuing a certificate after revocation 18
3.4. Subscriber's Identity Authentication for Certificate Revocation 18
4. Certificate Life-Cycle Operational Requirements 18
4.1. Application Submission 18
4.1.1. Who can apply for certificate 18
4.1.2. Application process and related responsibilities 18
4.2. Applications processing 19
4.2.1. Identification and authentication function 19
4.2.2. Acceptance or rejection of application 19
4.2.3. Certificate Issuance Awaiting 20
4.3. Certificates Issuance 20
4.3.1. Authority activities during certificate issuance 20
4.3.2. Service recipient notification of certificate issuance 20
4.3.3. Certificate acceptance 20
4.3.4. Certificate publication 20
4.3.5. Informing other entities about certificate issuance 21
4.4. Certificate and Key Usage 21
4.4.1. Service recipients certificates and keys usage 21
4.4.2. Relying parties certificates and keys usage 21
4.5. Recertification 21
4.5.1. Circumstances for certificate recertification 21
4.5.2. Who can apply for certificate recertification 21
4.5.3. Recertification application processing 21
4.5.4. Informing subscriber about certificate issuance 21
4.5.5. Acceptance of a recertification of certificate 21
4.5.6. Recertification of certificate publication 22
4.5.7. Informing other entities about certificate issuance 22
4.6. Certification and rekey (key update) 22
4.6.1. Circumstance for Certification and Rekey 22
4.6.2. Who can apply for a new public key 22
4.6.3. Application for certification and rekey processing 22
4.6.4. Informing subscriber about new certificate issuance 22

4.6.5. Acceptance of new certificate 22
4.6.6. New certificate publication 22
4.6.7. Informing other entities about certificate issuance 22
4.7. Certificate data modification 22
4.7.1. Circumstance for certificate data modification 22
4.7.2. Who can apply for a certificate data modification 22
4.7.3. Certificate Data Modification Requests Processing 22
4.7.4. Informing subscriber about certificate data modification 23
4.7.5. Acceptance of modified data certificate 23
4.7.6. Modified data certificate publication 23
4.7.7. Informing other entities about certificate issuance 23
4.8. Certificate revocation and suspension 23
4.8.1. Circumstances for certificate revocation 23
4.8.2. Who can request certificate revocation 23
4.8.3. Procedure for certificate revocation 23
4.8.4. Certificate revocation grace period 24
4.8.5. Maximum time of processing revocation application 24
4.8.6. Obligatory revocation check 24
4.8.7. CRL issuance frequency 24
4.8.8. Maximum delay of publishing Certificate Revocation List 24
4.8.9. On-line certificate status verification availability 24
4.8.10. Wymagania sprawdzania unieważnień w trybie on-line 24
4.8.11. Other forms of revocation advertisements availability 24
4.8.12. Special duties in case of rekey security breach 25
4.8.13. Circumstances of certificate suspension 25
4.8.14. Who can request certificate suspension 25
4.8.15. Procedure of certificate suspension and unsuspension 25
4.8.16. Limitation on suspension grace period 25
4.8.17. Revocation or suspension of the Trusted Service Provider certificate 25
4.9. Other services – Certificate status services 25
4.9.1. Operational characteristics 25
4.9.2. Services availability 25
4.9.3. Optional functions 25
4.10. End of subscription 25
4.11. Key escrow and restoration 25
4.11.1. Principles and of key escrow and restoration 25
4.11.2. Session key encapsulation, restoration policy and practice 26

5. Facilities, Management and Operational Controls 26
5.1. Physical security controls 26
5.1.1. Site location and construction 26
5.1.2. Physical access 26
5.1.3. Power and air conditioning 26
5.1.4. Water exposure 26
5.1.5. Fire prevention 26
5.1.6. Media storage 26
5.1.7. Waste disposal 26
5.1.8. Offsite backup storage 26
5.1.9. Registration authority security controls 26
5.2. Organizational security controls 27
5.2.1. Trusted roles 27
5.2.2. Numbers of persons required per task 27
5.2.3. Identification and Authentication for Each Role 28
5.2.4. Roles that cannot be combined 28
5.3. Personnel controls 28
5.3.1. Qualifications, experience and authorization 28
5.3.2. Personnel verification procedure 28
5.3.3. Training requirements 28
5.3.4. Retraining Frequency and Requirements 28
5.3.5. Job rotation 28
5.3.6. Sanctions for Unauthorized Actions 28
5.3.7. Contract Personnel 28
5.3.8. Documentation Supplied to Personnel 28
5.4. Events recording, security incidents management and audit procedures 28
5.4.1. Types of events recorded 28
5.4.2. Frequency of event logs checking 29
5.4.3. Event journals retention period 29
5.4.4. Protection of event logs 29
5.4.5. Procedures for event logs backup 29
5.4.6. Collecting data for internal and external audit 29
5.4.7. Notification to event responsible entities 29
5.4.8. Vulnerability assessment 29
5.5. Records archival 29
5.5.1. Types of data archived 29
5.5.2. Archive retention period 29

5.5.3. Archive protection 29
5.5.4. Backup procedures 29
5.5.5. Requirements for electronically timestamping of the records 29
5.5.6. Collecting of archival data (internal and external) 29
5.5.7. Procedures to obtain and verify archive information 30
5.6. Key changeover 30
5.7. Key security violation and disaster recovery 30
5.7.1. Procedures for handling incidents and respond to threats 30
5.7.2. Computing resources, software, and/or data are corrupted 30
5.7.3. Key compromise or suspicion of certification authority private key compromise 30
5.7.4. Business continuity capabilities after a disaster 30
5.8. Certification authority termination or service transition 30
5.8.1. Requirements associated with duty transition 30
5.8.2. Dealing with a terminated certification authority 30
6. Technical Security Controls 30
6.1. Generowanie pary kluczy i jej instalowanie 30
6.1.1. Key pair generation and installation 30
6.1.2. Private Key Delivery to Entity 31
6.1.3. Public Key Delivery to certification authority 31
6.1.4. Certification authority public key delivery to relying parties 31
6.1.5. Keys Sizes 31
6.1.6. Public Key Generation Parameters and quality checking 31
6.1.7. Key Usage Purposes 32
6.1.8. Hardware and/or Software Key Generation 32
6.2. Private key protection 32
6.2.1. Standards for Cryptographic Modules 32
6.2.2. Private Key Multi-Person Control 32
6.2.3. Private Key Escrow 32
6.2.4. Private Key Backup 32
6.2.5. Private Key Archival 32
6.2.6. Private Key Entry into Cryptographic Module 33
6.2.7. Private Key Storage in Cryptographic Module 33
6.2.8. Method of Activating Private Key 33
6.2.9. Method of Deactivating Private Key 33
6.2.10. Method of Destroying Private Key 33
6.2.11. Cryptographic Modules ratings 33
6.3. Other Aspects of Key Pair Management 33

6.3.1. Public Key Archive 33
6.3.2. Usage Periods of Public and Private Keys 33
6.4. Activation Data 33
6.4.1. Activation Data Generation and Installation 33
6.4.2. Activation Data Protection 34
6.4.3. Other Aspects of Activation Data 34
6.5. Computer Security Controls 34
6.5.1. Specific Computer Security Technical Requirements 34
6.5.2. Computer Security Rating 34
6.6. Technical control 34
6.6.1. System Development Controls 34
6.6.2. Security Management Controls 34
6.6.3. Life Cycle Security Ratings 34
6.7. Network Security Controls 34
6.8. Electronic Timestamps as a security control 34
7. Certificate, CRL, and OCSP Profile 34
7.1. Certificate Profile 35
7.1.1. Certificate content 35
7.1.2. Version number 36
7.1.3. Certificate Extensions and issued certificates or trust service providers certificates types 36
7.1.4. Electronic signature algorithm identifier 38
7.1.5. Name forms 38
7.1.6. Names restrictions 38
7.1.7. Certification Policy Identifiers 38
7.1.8. Certification Policy Identifiers Extensions usage on defining politics restrictions 38
7.1.9. Policy qualifiers syntax and semantics 38
7.1.10. Processing semantics critical extension of the certification policy 38
7.2. CRL profile 38
7.2.1. Version number 39
7.2.2. Supported CRL entry extension 39
7.2.3. Revoked certificates and CRL 39
7.3. OCSP profile 39
7.3.1. Version number 39
7.3.2. Supported Extensions 39
7.4. Other profiles 39
7.4.1. Electronic timestamp token profile 39

7.4.2. Qualified validation tokens profiles 39
7.4.3. OCSP response token profiles 39
8. Compliance audit 39
8.1. Audit Frequency 39
8.2. Identity/Qualifications of the Auditor 39
8.3. Auditor relationship with audited entity 39
8.4. Topics Covered under the Compliance Audit 40
8.5. Actions Taken as a Result of Deficiency 40
8.6. Notifying of Audit Results 40
9. Other Business and Legal Matters 40
9.1. Fees 40
9.1.1. Certificate issuance fees 40
9.1.2. Certificates and trust service providers certificate access fees 40
9.1.3. Qualified certificate revocation and status information access fees 40
9.1.4. Other Fees 40
9.1.5. Fees Refund 40
9.2. Financial Responsibility 40
9.2.1. Insurance coverage 40
9.2.2. Other assets 41
9.2.3. Extended warranty coverage 41
9.3. Confidentiality of business information 41
9.3.1. Types of Information to be Kept Secret 41
9.3.2. Types of Information Not Considered Confidential and Private 41
9.3.3. Obligation to protect confidentiality of information 41
9.4. Privacy of Personal Information 41
9.4.1. Privacy Policy 41
9.4.2. Information considered as private 41
9.4.3. Information not considered as private 41
9.4.4. Responsibility to protect private information 41
9.4.5. Reservations and permission to use private information 41
9.4.6. Sharing information in accordance with a court order or administrative 41
9.4.7. Other circumstances disclosure 41
9.5. Intellectual Property Rights 42
9.5.1. Trade Mark 42
9.6. Commitments and guarantees 42
9.6.1. Certum’s obligations and guarantee 42
9.6.2. Registration authorities obligations and guarantees 42

9.6.3. Subscriber obligations and guarantees 42
9.6.4. Relying Party Obligations and Guarantees 42
9.6.5. Other Users Obligations and Guarantees 42
9.7. Warranty Disclaimer 42
9.8. Liability 42
9.8.1. Certum liability 42
9.9. Compensations 43
9.9.1. Subscribers civil liability compensation 43
9.9.2. Relying party civil liability compensation 43
9.10. Certificate Policy and Certification Practice Statement validity period 43
9.10.1. Validity period 43
9.10.2. Expiration 43
9.10.3. Certificate Policy and Certification Practice Statement expiry effects 43
9.11. Users notification and communication 43
9.12. Changes introduction procedure 44
9.12.1. Modification introduction procedure 44
9.12.2. Notification mechanism of and comment period 44
9.12.3. Changes requiring new identifier 44
9.12.4. Publication of the new version of Certificate Policy and Certification Practice Statement and Terms & Conditions for Qualified Trust Services 44
9.12.5. Items not published in Certificate Policy and Certification Practice Statement 44
9.13. Disputes Resolution, complaints 44
9.14. Governing law 44
9.14.1. Resolution Survival 44
9.14.2. Provision references 44
9.15. Accordance with applicable law 44
9.16. Other laws 44
9.16.1. Contracts completeness 45
9.16.2. Conveyance 45
9.16.3. Resolution severability 45
9.16.4. Enforcement clause 45
9.16.5. Force majeure 45
9.17. Additional provisions 45
9.17.1. Other Certum Policies 45
10. Document History 46
11. Glossary 47

1. Introduction

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

These services are provided in accordance with:

- the Integrated Management System, implemented by Asseco Data Systems S.A., which includes the requirements of the PN-EN ISO 9001:2009 and PN-ISO/IEC 27001:2014,
- the *Regulation of the Ministry of Digitalisation of 5th October 2016 according the National Trust Infrastructure,*
- *the Act on Trust Services and Electronic Identification (Dz.U. 2019 r. poz. 162),*
- standards referred to in the Decision of the Executive Committee (EU) 2016/650 of 25 April 2016 establishing standards for assessment of the safety devices for qualified signature and stamp on the basis of art. 30 paragraph 3 and art. 39 paragraph 2 *Regulation of the European Parliament and of the Council (EU) No 910/2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93/EC*, hereinafter called *the eIDAS Regulation*,
- the service mentioned above in point 1, i.e.: the service of issuing qualified certificates in the signing process is provided in accordance with with the requirements of the *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, hereinafter referred to as the *eIDAS Regulation*.

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

The applicability ranges of qualified certificates issued in the signing process, issued in accordance with this document are described in chapter 1.4. , and the liability resulting from their use by Certum and end-users - in chapter 9.8.

The structure and contents of CISP Policy is in accordance with the recommendation of RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. It also fulfils the requirements of the ETSI EN 319 411-1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* and requirements of the standard ETSI EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates* norms.

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

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

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

1.1. Overview

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

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

1.2. Document Name and its Identification

The present document is given a proper name of **Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service - certificate issued in the signing process**, and is available in an electronic version at: www.certum.eu.

The following registered object identifier is connected with the above-mentioned document (OID: 1.2.616.1.113527.2.4.1.0.3.1.2)[2]:

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-cisp(3) version(1) 2}

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

1.3. CISP Policy Parties

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

- Certum's Certification Authorities,
- Primary Registration Authority (PRA),
- Registration Authorities (RA),
- persons confirming the identity,
- subscribers,
- relying parties.

An important element to emphasize is the fact that within the framework of Registration Authorities (RA) it is possible to operate the so-called **Business Identity Confirmation Points**,

[2] The CISP Policy document identifier should not be confused with the certification policy identifier (the so-called OID identifier), placed in the content of the issued certificate (see chapter 1.3.1.1).

hereinafter referred to as BICP, and **Business Partners** (e.g. banking or leasing facilities), the nature, scope and openness of operation of which depends on the adopted business model between Certum and a given Business Partner.

1.3.1. Trust Services Authorities

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

1.3.1.1. Qualified Certification Authority Certum QCA 2017

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

1.3.1.2. Qualified Electronic Timestamp Authority Certum QTST 2017

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

1.3.1.3. Qualified online certificate status protocol authority CERTUM QOCSP

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

1.3.1.4. Qualified Validation Service for qualified electronic signatures and qualified electronic seals CERTUM QDVCS and Certum QESValidationQ 2017

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

1.3.2. Primary Registration Authority, Registration authorities and points of the identity verification

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

In addition, Business Identity Confirmation Points and Business Partners operate on the principles set out in the Main Policy.

1.3.3. Subscribers

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

1.3.4. Relying Parties

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

1.3.5. Other Parties

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

1.4. Certificate and certificate of trust service provider usage

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

1.4.1. Types of certificates and trust services provider certificates and recommended areas of application

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

1.4.1.1. Qualified certificates

As part of this CISP Policy, qualified personal (universal) electronic signature certificates are issued.

Information on the types of certificates and their applications has been addressed in the Main Policy.

1.4.1.2. Trust service providers certificate

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

1.4.1.3. Electronic timestamps

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

1.4.1.4. OCSP Response Tokens Applicability Range

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

1.4.1.5. Data Validation Applicability Range

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

1.4.2. Prohibited Certificate Uses

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

1.5. Certificate Policy and Certification Practice Statement Administration

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

1.5.1. Organization responsible for administrating the document

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

1.5.2. Contact

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

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

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

1.5.4. Approval Procedures

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

1.6. Definitions and abbreviations

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

2. Publication and Repository

2.1. Repository

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

2.2. Information Published by Certum

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

2.3. Frequency of Publication

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

2.4. Access to Publications

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

3. Identification and Authentication

The general rules of subscribers' identity verification applied by Certum in the scope of issuing qualified certificates are specified in the Main Policy.

The rules specifying the types of information included in the content of the qualified certificate, and the measures to be taken in order to ensure that this information is accurate and reliable at the time of issuing the certificate remain unchanged.

The verification is **obligatorily** performed in the stage of subscriber’s registration, which in case of the CISP Policy, is related to the client's business process.

3.1. Naming

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

3.1.1. Types of Names

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

3.1.2. Need for Names to be Meaningful

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

Certificates issued in accordance with this CISP Policy are issued in Category I.

3.1.3. Subscribers anonymity

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

3.1.4. Rules for Interpreting Various Names Forms

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

3.1.5. Names Uniqueness

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

3.1.6. Recognition, Authentication and Role of Trademarks

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

3.2. Initial Registration

Registration comprises of a number of internal procedures which allow a registration system point, prior to issuing a certificate for qualified electronic signature to a service recipient, to gather authenticated data about the entity, identifying its identity and rights. Confirmation of these data may be carried out in accordance with art. 24.1 of the *eIDAS Regulation*.

Service recipient submits an application (Statement) that confirms the accuracy of his/hers data and consent to assign this data to him/her. On the basis of this request, Certum issues a certificate.

Accuracy of the data contained in the application (Statement) for a new certificate is confirmed in the identity verification process described in Section 3.2.3.1

Statement is signed electronically by the service recipient using an Advanced Electronic Signature or Advanced Electronic Seal.

Certificate is an electronic attestation that contains identification data of the service recipient and data used to verify the authenticity of the electronic signature. Electronic signature is made by means of data contained (stored) in the hardware cryptographic module (HSM), over the use of which only the customer has control through exclusive control over the mobile phone, on which he/she will receive a code allowing to use this data to create signature.

Service recipient is obliged to confirm that he/she has read the "Terms & Conditions for Certum Qualified Trust Service - certificate issued in the signing process" by accepting the terms of provision of trust service.

3.2.1. Proof of Possession of Private Key

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

3.2.2. Authentication of the subscriber's rights and other attributes

Not applicable.

3.2.3. Authentication of natural person's identity

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

3.2.3.1. Identity verification by an authorized representative of Certum

The service recipient's identity is confirmed on the basis of a valid identity card or passport via the Business Identity Confirmation Point. Confirmation of the service recipient's identity can be done in two ways:

- through personal appearance at a Business Identity Confirmation Point,
- remotely, by a third-party provider using means to confirm the identity subscriber in a manner that provides credibility equivalent to physical presence, through methods described in Article 24.1 of the eIDAS Regulation.

If the Identity Confirmation Point is operated by a Partner that is a financial sector entity required under the provisions of the Directive of the European Parliament and of the Council (EU) 2015/849 (AML) and applies a sufficiently high level of reliability to verify the identity of individuals, the operator of this point may use the identity verification methods used by this entity. While always:

- process must be accurately described in the procedure and approved by Certum,
- an up-to-date risk analysis must be provided for the process used, with particular attention to the risks of identity impersonation,
- Partner must implement the requirements of Article 24.2 of the eIDAS Regulation (to the extent that they apply to it),
- Partner must declare its willingness to verify compliance with the requirements in the form of an audit by Certum's internal auditors or external auditors.

3.2.3.2. Identity verification using a video-identification system

In accordance with Article 24.1 of the eIDAS Regulation.

3.2.3.3. Identity verification by a notary public

Not applicable.

3.2.3.4. Identity verification based on a qualified electronic signature

In accordance with Article 24.1 of the eIDAS Regulation.

3.2.3.5. Identity verification using an electronic identification means

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

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

Not applicable.

3.2.6. Interoperability criteria

Not applicable.

3.3. Subscriber's Identity Authentication for Certificate Rekey or Certificate Data Modification requests

Not applicable.

3.3.1. Identification and authentication in a standard rekey

Not applicable.

3.3.1.1. Certification and Rekey

Not applicable.

3.3.1.2. Certificate Data Modification

Not applicable.

3.3.2. Authentication for issuing a certificate after revocation

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

3.4. Subscriber's Identity Authentication for Certificate Revocation

Revocation requests can be submitted by phone.

Validation service recipient's identity and the request for certificate revocation is carried out at the Primary Registration Authority by the Registration Inspector.

A detailed description of certificate revocation procedure can be found in chapter 4.8.3.

4. Certificate Life-Cycle Operational Requirements

The method of certificate issuance in the signing process service is presented below. Certificate issuance begins with the service recipient submitting an appropriate application in the Business Identity Confirmation Point. The submitted applications should contain information that is necessary to correctly identify the service recipient and the data contained in the submitted application.

4.1. Application Submission

4.1.1. Who can apply for certificate

Any natural person who is or will be the subject of the certificate may apply for a certificate. The application must be authenticated by an authorized representative of Certum, in this case the operator of the Business Identity Confirmation Point.

Certum does not issue certificates to business entities in countries with which the law of the Republic of Poland prohibits trading.

4.1.2. Application process and related responsibilities

4.1.2.1. Certification Application

Application for certification is submitted by the customer to Business Identity Confirmation Point. It is entered into the system by the BICP operator.

4.1.2.2. Certificate rekey or certificate data modification application

Not applicable.

4.1.2.3. Certificate revocation or suspension application

An application for certificate revocation can be submitted by phone call.

Applications must be confirmed by registration inspector.

The scope of information that must be provided during the phone call is as follows:

- Name and surname of the service recipient,
- Service recipient's telephone number,
- Certificate serial number,
- The signing code.

Service recipient is informed about certificate revocation by means of an SMS text message sent to the telephone number provided in the certificate application.

4.2. Applications processing

After identity validation of the service recipient in accordance with chapter 3.2, certification application is sent to Certum in order to issue a certificate.

4.2.1. Identification and authentication function

Identification and authentication functions of all required service recipient's data are performed by the Primary Registration Point and cooperating Business Identity Confirmation Points in accordance with the conditions specified in chapter 1.3.2.

4.2.2. Acceptance or rejection of application

4.2.2.1. Application processing

Business Identity Confirmation Point accepts and verifies the certificate application and submits it to the Primary Registration Point.

4.2.2.2. Rejection of certificate issuance

Certum may refuse to issue a certificate to any service recipient without incurring any obligations or exposing itself to any liability which may arise as a result of losses or costs incurred by the service recipient (as a result of the refusal). In such a case, Certum returns to the service recipient the fee paid by him/her for issuing the certificate (if he/she made an appropriate prepayment), unless the service recipient stated false or untrue data in his/hers certificate declaration.

The refusal to certificate issuance may occur in the following cases:

- session during which the certificate issued in the signing process was to be issued has expired,
- the service recipient has entered the wrong signature authorization code for the third time,

- data in the Statement is inconsistent with the facts,
- a breach of obligations by the Business Partner resulting from non-compliance with Certum procedures has been found.

Refusal to issue a certificate - when Certum receives data on the basis of which the Statement is generated:

- confirmation of non-compliance of data in the Statement with the facts,
- confirmation of breach of the obligations of the "partner" resulting from non-compliance with Certum procedures.

4.2.3. Certificate Issuance Awaiting

Certificate is issued immediately from the moment of submitting a correctly filled and verified application.

4.3. Certificates Issuance

Service recipient accepts the issuance of the certificate by using an acceptance code.

4.3.1. Authority activities during certificate issuance

Certification authority verifies the application, and after confirming its correctness, issues a certificate.

Each certificate is issued in a closed internal zone of Asseco Data Systems S.A., to which there is no access from the global network.

4.3.2. Service recipient notification of certificate issuance

Operator of the Business Identity Confirmation Point handling the application or Certum's system informs the service recipient about the issuance of the certificate immediately after its issuance.

The moment of signing with one-time signature, for which a certificate was issued in the signing process, is the moment when the service recipient receives his/hers certificate.

4.3.3. Certificate acceptance

Certificate acceptance is carried out as part of the business process in which the recipient participates, by verifying and accepting data (name, surname, ID document number) and signing of the Statement with service recipient's data, which will be included in the certificate, for which exact reflection in the generated certificate Certum is responsible. The remaining information included in the certificate is the technical information for which Certum is responsible.

Certificate acceptance is also unequivocal to the service recipient's declaration that before using the public key contained in the certificate or the private key complementary to it in any cryptographic operation, he/she carefully read the terms of provision of provided by Asseco Data Systems S.A. trust service concluded during the registration procedure at the registration system point.

4.3.4. Certificate publication

Not applicable.

4.3.5. Informing other entities about certificate issuance

Not applicable.

4.4. Certificate and Key Usage

4.4.1. Service recipients certificates and keys usage

Service recipients are required to use private key and certificates::

- in accordance with their purpose stated in the present CISP Policy and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage** see chapter 7.1),
- in accordance with the content of accepted by service recipient terms of provision of trust services by Asseco Data Systems S.A.,
- only within the validity period,
- until the moment of certificate revocation.

Certum verifies whether the certificate associated with the private key of the service recipient is valid at the time of signing.

4.4.2. Relying parties certificates and keys usage

Relying parties must use public keys and certificates:

- in accordance with their purpose stated in the present CISP Policy and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage** see chapter 7.1),
- only upon their status verification.

4.5. Recertification

Not applicable.

4.5.1. Circumstances for certificate recertification

Not applicable.

4.5.2. Who can apply for certificate recertification

Not applicable.

4.5.3. Recertification application processing

Not applicable.

4.5.4. Informing subscriber about certificate issuance

Not applicable.

4.5.5. Acceptance of a recertification of certificate

Not applicable.

4.5.6. Recertification of certificate publication

Not applicable.

4.5.7. Informing other entities about certificate issuance

Not applicable.

4.6. Certification and rekey (key update)

Not applicable.

4.6.1. Circumstance for Certification and Rekey

Not applicable.

4.6.2. Who can apply for a new public key

Not applicable.

4.6.3. Application for certification and rekey processing

Not applicable.

4.6.4. Informing subscriber about new certificate issuance

Not applicable.

4.6.5. Acceptance of new certificate

Not applicable.

4.6.6. New certificate publication

Not applicable.

4.6.7. Informing other entities about certificate issuance

Not applicable.

4.7. Certificate data modification

Not applicable.

4.7.1. Circumstance for certificate data modification

Not applicable.

4.7.2. Who can apply for a certificate data modification

Not applicable.

4.7.3. Certificate Data Modification Requests Processing

Not applicable.

4.7.4. Informing subscriber about certificate data modification

Not applicable.

4.7.5. Acceptance of modified data certificate

Not applicable.

4.7.6. Modified data certificate publication

Not applicable.

4.7.7. Informing other entities about certificate issuance

Not applicable.

4.8. Certificate revocation and suspension

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

Certum does not use the certificate suspension procedure for a certificate issued in the signing process.

4.8.1. Circumstances for certificate revocation

In case of certificates issued in accordance with the CISP Policy, the issued certificates may be revoked in two cases:

- when service recipient resigns from signing the documents he/she was supposed to sign using the issuing qualified certificates in the signing process service;
- when verifying the content of the issued certificate, the service recipient finds that the certificate contains incorrect data.

4.8.2. Who can request certificate revocation

Certificate request revocation may be submitted by:

- a service recipient whose data is included in the certificate,
- an authorized representative of a certification authority (in the case of Certum this role is reserved for the security inspector),
- Minister of Digital Affairs.

4.8.3. Procedure for certificate revocation

The request for certificate revocation may be submitted by phone.

By calling the number: +48 91 4801 360, the service recipient submits an application for certificate revocation. For the application to be successfully submitted, the recipient must provide the following information:

- name and surname of the service recipient,
- telephone number of the service recipient (which he/she provided in the certificate application),
- signing code,
- certificate serial number.

The registration inspector who received the revocation application verifies the request. In case of positive verification, the certificate shall be revoked within 24 hours from the moment of accepting the application. Information about the revoked certificate is available in the OCSP service.

In case of negative verification, the certificate will not be revoked.

Revoked certificate and the private key complementary to it, stored in the hardware cryptographic module (HSM), are irreversibly removed from this carrier. The operation is performed automatically during the realization of request for certificate revocation, approved by the registration inspector.

4.8.4. Certificate revocation grace period

Certum guarantees that the maximum delay period in the processing of certificate revocation request is 24 hours.

4.8.5. Maximum time of processing revocation application

Certificate revocation request is processed by Certum within 24 hours from reception of the request.

4.8.6. Obligatory revocation check

The relying party, upon receiving the electronic document signed by the service recipient is obliged to check in the OCSP service whether the public key certificate corresponding to the private key with which the service recipient performed the signature has not been revoked.

Certum guarantees uninterrupted access to certificate's status information for 24/7 (24 hours / 7 days a week).

4.8.7. CRL issuance frequency

Certum does not publish CRLs for certificates issued in accordance with this Policy.

4.8.8. Maximum delay of publishing Certificate Revocation List

Not applicable.

4.8.9. On-line certificate status verification availability

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

Certum does not publish CRLs for certificates issued in accordance with this Policy.

4.8.10. Wymagania sprawdzania unieważnień w trybie on-line

A relying party is not obligated to verify certificate status *on-line* on the basis of mechanisms and services laid down in chapter 4.8.9. On-line certificate status verification availability However, it is recommended to use this option when the risk of accepting an invalid or forged signature is high.

4.8.11. Other forms of revocation advertisements availability

Not applicable.

4.8.12. Special duties in case of rekey security breach

Not applicable.

4.8.13. Circumstances of certificate suspension

This policy does not allow certificate suspension.

4.8.14. Who can request certificate suspension

Not applicable.

4.8.15. Procedure of certificate suspension and unsuspension

Not applicable.

4.8.16. Limitation on suspension grace period

Not applicable.

4.8.17. Revocation or suspension of the Trusted Service Provider certificate

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

4.9. Other services – Certificate status services

4.9.1. Operational characteristics

4.9.1.1. Electronic timestamp service

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

4.9.1.2. Qualified Validation Service for qualified electronic signatures and qualified electronic seals

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

4.9.2. Services availability

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

4.9.3. Optional functions

Not applicable.

4.10. End of subscription

Not applicable.

4.11. Key escrow and restoration

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

4.11.1. Principles and of key escrow and restoration

Not applicable.

4.11.2. Session key encapsulation, restoration policy and practice

Not applicable.

5. Facilities, Management and Operational Controls

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

5.1. Physical security controls

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

5.1.1. Site location and construction

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

5.1.2. Physical access

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

5.1.3. Power and air conditioning

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

5.1.4. Water exposure

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

5.1.5. Fire prevention

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

5.1.6. Media storage

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

5.1.7. Waste disposal

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

5.1.8. Offsite backup storage

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

5.1.9. Registration authority security controls

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

5.1.9.1. Site location and construction

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

5.1.9.2. Physical access

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

5.1.9.3. Power and air conditioning

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

5.1.9.4. Water exposure

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

5.1.9.5. Fire prevention and protection

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

5.1.9.6. Media storage

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

5.1.9.7. Waste disposal

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

5.1.9.8. Offsite archive storage

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

5.1.10. Service recipient security

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

5.2. Organizational security controls

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

5.2.1. Trusted roles

5.2.1.1. Trusted roles in Certum

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

5.2.1.2. Trusted roles in registration authority

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

5.2.1.3. Subscriber's trusted roles

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

5.2.2. Numbers of persons required per task

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

5.2.3. Identification and Authentication for Each Role

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

5.2.4. Roles that cannot be combined

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

5.3. Personnel controls

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

5.3.1. Qualifications, experience and authorization

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

5.3.2. Personnel verification procedure

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

5.3.3. Training requirements

BICP operators must be trained in the identity validation procedure and the operation of certificate issuance in the signing process system. If the BICP has undergone training in the field of identity validation in his/hers organization and the scope of the training fully covers the scope of training provided by Certum (e.g. training provided by banks for their operators), no separate training is required by Certum.

5.3.4. Retraining Frequency and Requirements

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

5.3.5. Job rotation

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

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Contract Personnel

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

5.3.8. Documentation Supplied to Personnel

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

5.4. Events recording, security incidents management and audit procedures

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

5.4.1. Types of events recorded

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

5.4.2. Frequency of event logs checking

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

5.4.3. Event journals retention period

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

5.4.4. Protection of event logs

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

5.4.5. Procedures for event logs backup

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

5.4.6. Collecting data for internal and external audit

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

5.4.7. Notification to event responsible entities

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

5.4.8. Vulnerability assessment

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

5.5. Records archival

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

5.5.1. Types of data archived

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

5.5.2. Archive retention period

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

5.5.3. Archive protection

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

5.5.4. Backup procedures

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

5.5.5. Requirements for electronically timestamping of the records

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

5.5.6. Collecting of archival data (internal and external)

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

5.5.7. Procedures to obtain and verify archive information

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

5.6. Key changeover

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

5.7. Key security violation and disaster recovery

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

5.7.1. Procedures for handling incidents and respond to threats

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

5.7.2. Computing resources, software, and/or data are corrupted

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

5.7.3. Key compromise or suspicion of certification authority private key compromise

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

5.7.4. Business continuity capabilities after a disaster

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

5.8. Certification authority termination or service transition

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

5.8.1. Requirements associated with duty transition

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

5.8.2. Dealing with a terminated certification authority

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

6. Technical Security Controls

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

6.1. Generowanie pary kluczy i jej instalowanie

6.1.1. Key pair generation and installation

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

6.1.1.1. Key pair generation

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

6.1.1.1.1 Procedures of generation of Certum initial keys

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

6.1.1.1.2 Certification authority keys re-key procedures

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

6.1.2. Private Key Delivery to Entity

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

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

Qualified service recipients - a certificate issued in the signing process receive access to personalized virtual cards placed on a hardware cryptographic module. Card personalization means preparing the card for use by establishing the main structure of the card, creating profiles, generating a unique card number. The card created in this way acts as a safe device on which the service recipient's certificate will be located. Card personalization process takes place in a secure room - which is accessible only to employees who act as the trusted roles - service recipient's cryptographic keys and card identification numbers are generated on cards and automatically saved to database. Card personalization is performed on devices not connected to the network.

Data for card activation, i.e. code sent via SMS, needed to create the electronic signature, is made available to service users regardless of the issued certificates.

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

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

6.1.3. Public Key Delivery to certification authority

Not applicable.

6.1.4. Certification authority public key delivery to relying parties

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

6.1.5. Keys Sizes

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

6.1.6. Public Key Generation Parameters and quality checking

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

6.1.7. Key Usage Purposes

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

6.1.8. Hardware and/or Software Key Generation

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

6.2. Private key protection

Service recipient's keys are generated and maintained in a hardware cryptographic module. Certification authority (see chapter 6.1.1. Key pair generation and installation), which generates the key pair on behalf of the service recipient, must securely provide access to the key pair and instruct the service recipient on the principles of private key protection (see chapter 6.1.2. Private Key Delivery to Entity).

6.2.1. Standards for Cryptographic Modules

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

6.2.2. Private Key Multi-Person Control

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

6.2.2.1. Acceptance of secret shares by its holders

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

6.2.2.2. Protection of secret shares

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

6.2.2.3. Availability and erasure (transfer) of shared secret

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

6.2.2.4. Responsibilities of shared secret holder

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

6.2.3. Private Key Escrow

Private keys of service recipients are stored on a hardware cryptographic module and are only available to the service recipient after using the code received via SMS, in accordance with the internal Certum procedure.

6.2.4. Private Key Backup

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

Certum does not retain copies of service recipients private keys..

6.2.5. Private Key Archival

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

6.2.6. Private Key Entry into Cryptographic Module

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

6.2.7. Private Key Storage in Cryptographic Module

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

6.2.8. Method of Activating Private Key

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

Service recipients private keys of are activated only after authentication (providing the code received via SMS) and only for duration of the electronic signature creation with the use of this key. After performing the operation, the private key is automatically removed from the hardware cryptographic module.

6.2.9. Method of Deactivating Private Key

Not applicable.

6.2.10. Method of Destroying Private Key

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

6.2.11. Cryptographic Modules ratings

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

6.3. Other Aspects of Key Pair Management

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

6.3.1. Public Key Archive

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

6.3.2. Usage Periods of Public and Private Keys

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

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

6.4. Activation Data

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

6.4.1. Activation Data Generation and Installation

Signature creation is activated by the service recipient who has control over the entire process by having a mobile phone under his/her sole control. On this phone, he/she will receive a code via

SMS that authorizes the use of the private key contained in the hardware cryptographic module for signature creation.

6.4.2. Activation Data Protection

The certainty that the authorization code will reach the service recipient is ensured by the personal appearance of the service recipient in BICP and the validation of recipient's identity by the BICP operator. Mechanism for delivering the code can also be implemented alternatively remotely by Certum systems using electronic communication.

6.4.3. Other Aspects of Activation Data

The authorization code cannot be changed.

6.5. Computer Security Controls

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

6.5.1. Specific Computer Security Technical Requirements

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

6.5.2. Computer Security Rating

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

6.6. Technical control

6.6.1. System Development Controls

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

6.6.2. Security Management Controls

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

6.6.3. Life Cycle Security Ratings

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

6.7. Network Security Controls

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

6.8. Electronic Timestamps as a security control

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

7. Certificate, CRL, and OCSP Profile

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

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

7.1. Certificate Profile

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

7.1.1. Certificate content

The content of the trust service provider's certificate is presented in the Main Policy (chapter 7.1.1, Tab.15).

Tab.1. Profile of basic fields of the service recipient's qualified certificate issued in the signing process

Field name	Value or value constraint	
Version	3	
Serial Number	Unique value for all certificate issued by qualified Certum QCA 2017 certification authority.	
Signature Algorithm	*sha512WithRSAEncryption* (OID: 1.2.840.113549.1.1.13)	
Issuer: Certum QCA 2017	Common Name (CN) =	Certum QCA 2017
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Organization Identifier (2.5.4.97) =	VATPL-5170359458
Subject: Service recipient	Common Name (CN)	Name and surname of the service recipient
	Given Name (G) =	Name of the service recipient
	Surename (SN) =	Surname of the service recipient
	Serial Number =	Service recipient's identity document identifier recorded in accordance with the requirements in ETSI EN 319 412-1 chapter 5.1.3
	Country (C; Kraj) =	Country of issuance of the service recipient's identity document

Field name	Value or value constraint	
Not before (validity period beginning date)	Universal Time Coordinated based. Certum owns satellite clock controlled by Atomic Frequency Standard. Certum clock is known as valid world Stratum I service.	
Not after (validity period ending date)		
Subject Public Key Info	Algorithm	RSA encryption *RSA encryption* (OID: 1.2.840.113549.1.1.1)
	Public Key length	2048 bits
	Public Key value	Value is expressed in the form of a string of bytes.
Signature	Certificate signature is generated and coded: • according to the "Signature algorithm" field, • by the Issuer in order to confirm the relationship of the public key with the Subject.	

7.1.2. Version number

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

7.1.3. Certificate Extensions and issued certificates or trust service providers certificates types

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

7.1.3.1. Qualified certificates

Tab.2. Standard extension fields of the service recipient's qualified certificate issued in the signing process

Extension	Value or Value constraint	Extension status
Authority Key Identifier	SHA-1 hash of the public key (OID: 2.5.29.35)	Non-critical
Subject Key Identifier	SHA-1 hash of the public key (OID: 2.5.29.14)	Non-critical
Basic Constraints	Subject type=empty (end entity) Path length constraint=none (OID: 2.5.29.19)	Critical
Key Usage	Digital Signature, bit 0 Content commitment[3], bit 1 (OID: 2.5.29.15)	Critical
Subject Alternative Name	Other name = msisdn_uuid@simplysign.onthefly.pl[4] (OID: 1.2.616.1.113527.2.200.1)	Non-critical
Authority Information Access	Online Certificate Status Protocol (OCSP) https://qca-2017.qocsp-certum.com (OID: 1.3.6.1.5.5.7.48.1) Certification Authority - issuer https://repository.certum.pl/qca_2017.cer (OID: 1.3.6.1.5.5.7.48.2)	Non-critical
QC Statements	A statement that the certificate is an european qualified certificate [5]: id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1) A statement that the private key associated with the certificate resides in a qualified signature creation device: id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4) Reference to the information on Certum QCA 2017 public key infrastructure: id-etsi-qcs-QcPDS (OID: 0.4.0.1862.1.5) EN: https://repository.certum.pl/PDS/Certum_QCA-PDS_EN.pdf PL: https://repository.certum.pl/PDS/Certum_QCA-PDS_PL.pdf Indication that the certificate is used for the purposes of electronic signatures: id-etsi-qct-esign (OID: 0.4.0.1862.1.6.1)	Non-critical

[3] In the ITU-T X.509 standard, this bit has been renamed from "nonRepudiation" to "contentCommitment"

[4] msisdn_uuid@simplysign.onthefly.pl value is not the actual email address. It is the name given to the service recipient by Certum, necessary to issue a certificate in the signing process. The "msisdn" element is the customer's telephone number, and the "uuid" element is a fragment of the unique certificate issuance transaction number in the signing process.

[5] It is a declaration by Asseco Data Systems S.A. that the issued qualified certificates comply with the requirements of the eIDAS Regulation and the Act. Asseco Data Systems S.A. in this way additionally declares compliance of the issued qualified certificates with the ETSI EN 319 422 specification. The Statement always contains the object identifier with the value: {itu-t (0) identified-organization (4) etsi (0) id-qc-profile (1862) 1 1}.

Extension	Value or Value constraint	Extension status
Certificate Policies	Certificate Policy (OID: 2.5.29.32) 1.2.616.1.113527.2.4.1.15.1, 0.4.0.194112.1.2 (qualified certificates for e-signature, HSM, short-termed, for a natural person) Qualified certification policy qualifier https://www.certum.pl/repozytorium (OID: 1.3.6.1.5.5.7.2.1)	Critical

7.1.3.2. Certificates of trust service providers

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

7.1.3.3. Cross-certification trust service providers certificates

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

7.1.4. Electronic signature algorithm identifier

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

7.1.5. Name forms

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

7.1.6. Names restrictions

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

7.1.7. Certification Policy Identifiers

Certum QCA 2017 certification authority issues qualified certificates in the signing process in accordance with the certification policy with the identifier:

Qualified certificates for electronic signature, HSM, short-termed - 1.2.616.1.113527.2.4.1.15.1

7.1.8. Certification Policy Identifiers Extensions usage on defining politics restrictions

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

7.1.9. Policy qualifiers syntax and semantics

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

7.1.10. Processing semantics critical extension of the certification policy

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

7.2. CRL profile

Certum does not publish CRLs for certificates issued in accordance with this Policy.

7.2.1. Version number

Not applicable.

7.2.2. Supported CRL entry extension

Not applicable.

7.2.3. Revoked certificates and CRL

Revocation of a qualified certificate issued in the signing process - not applicable.

Revocation of the trust service provider's certificates and their inclusion in the CRLs was addressed in the Main Policy.

7.3. OCSP profile

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

7.3.1. Version number

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

7.3.2. Supported Extensions

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

7.4. Other profiles

7.4.1. Electronic timestamp token profile

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

7.4.2. Qualified validation tokens profiles

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

7.4.3. OCSP response token profiles

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

8. Compliance audit

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

8.1. Audit Frequency

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

8.2. Identity/Qualifications of the Auditor

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

8.3. Auditor relationship with audited entity

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

8.4. Topics Covered under the Compliance Audit

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

8.5. Actions Taken as a Result of Deficiency

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

8.6. Notifying of Audit Results

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

9. Other Business and Legal Matters

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

In addition, it should be noted that all business issues related to the issuance of certificates in the signing process are regulated between Asseco Data Systems S.A. and BICP or a Business Partner.

9.1. Fees

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

9.1.1. Certificate issuance fees

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

9.1.2. Certificates and trust service providers certificate access fees

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

9.1.2.1. Timestamps and tokens fees

Not applicable.

9.1.3. Qualified certificate revocation and status information access fees

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

9.1.4. Other Fees

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

9.1.5. Fees Refund

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

9.2. Financial Responsibility

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

9.2.1. Insurance coverage

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

9.2.2. Other assets

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

9.2.3. Extended warranty coverage

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

9.3. Confidentiality of business information

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

9.3.1. Types of Information to be Kept Secret

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

9.3.2. Types of Information Not Considered Confidential and Private

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

9.3.3. Obligation to protect confidentiality of information

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

9.4. Privacy of Personal Information

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

9.4.1. Privacy Policy

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

9.4.2. Information considered as private

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

9.4.3. Information not considered as private

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

9.4.4. Responsibility to protect private information

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

9.4.5. Reservations and permission to use private information

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

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

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

9.4.7. Other circumstances disclosure

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

9.5. Intellectual Property Rights

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

9.5.1. Trade Mark

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

9.6. Commitments and guarantees

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

9.6.1. Certum's obligations and guarantee

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

9.6.1.1. Electronic timestamp authority obligations

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

9.6.1.2. Certificate status authority and data validation authority obligations

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

9.6.1.3. Repository Obligations

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

9.6.2. Registration authorities obligations and guarantees

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

9.6.3. Subscriber obligations and guarantees

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

9.6.4. Relying Party Obligations and Guarantees

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

9.6.5. Other Users Obligations and Guarantees

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

9.7. Warranty Disclaimer

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

9.8. Liability

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

9.8.1. Certum liability

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

9.8.1.1. Certification authority Certum QCA 2017 liability

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

9.8.1.2. Electronic timestamp authority liability

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

9.8.1.3. Online certificate status protocol authority, qualified validation service authority liability

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

9.8.1.4. Repository liability

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

9.8.1.5. Subscriber liability

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

9.8.1.6. Relying party liability

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

9.9. Compensations

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

9.9.1. Subscribers civil liability compensation

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

9.9.2. Relying party civil liability compensation

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

9.10. Certificate Policy and Certification Practice Statement validity period

9.10.1. Validity period

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

9.10.2. Expiration

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

9.10.3. Certificate Policy and Certification Practice Statement expiry effects

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

9.11. Users notification and communication

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

9.12. Changes introduction procedure

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

9.12.1. Modification introduction procedure

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

9.12.1.1. Items that can be changed without notification

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

9.12.2. Notification mechanism of and comment period

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

9.12.2.1. Comment period

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

9.12.3. Changes requiring new identifier

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

9.12.4. Publication of the new version of Certificate Policy and Certification Practice Statement and Terms & Conditions for Qualified Trust Services

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

9.12.5. Items not published in Certificate Policy and Certification Practice Statement

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

9.13. Disputes Resolution, complaints

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

9.14. Governing law

9.14.1. Resolution Survival

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

9.14.2. Provision references

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

9.15. Accordance with applicable law

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

9.16. Other laws

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

9.16.1. Contracts completeness

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

9.16.2. Conveyance

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

9.16.3. Resolution severability

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

9.16.4. Enforcement clause

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

9.16.5. Force majeure

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

9.17. Additional provisions

9.17.1. Other Certum Policies

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

Certum also provides qualified validation service and qualified preservation service described in “Qualified validation service and qualified preservation service of qualified electronic signatures and seals (Certum QESValidationQ) Policy”.

10. Document History

Document modification history		
1.1	July 27th 2021	Preparation of English version of document
1.2	October 27th 2023	Expanding identity verification methods to include remote identification and verification using an electronic identification means.

11. Glossary

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

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

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

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

Signature authorizing code - a code sent via SMS, the introduction of which authorizes the use of the private key contained in the hardware cryptographic module (HSM) to create an electronic signature.