Updated April 2019 to match BR version 1.6.4

CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

1) Certum
2) Certum's non-qualified certification services forms a separate certification domains: certum and its root certification authority Certum CA and ctnDomena domain and its root certification authorities Certum Trusted Network CA, Certum Trusted Network CA 2, Certum Elliptic Curve CA, Certum Trusted Root CA and Certum EC-384 CA. Currently, there are several certification authorities subordinate to Certum CA, there are all listed in CPS, 3) BR version 1.6.6
4) Certification Policy of Certum's Certification Services v. 4.4, effective date:21.02.2019 http://certum.eu/certum/cert,expertise_certyfication_policy.xml Certification Practice Statement of Certum's Certification Services v. 6.3, effective date 18.11.2019 http://certum.eu/certum/cert,expertise_practice_statement.xml

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	Certification Policy of Certum's Certification Services, effective date: 21.02.2019 Certification Practice Statement effective date: 18.11.2019	
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*		
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	CPS chapter 1.3.2	The Primary Registration Authority receive, verify and approve or reject applications for registration, issuance, rekey, renewal, or evocation of the certificate. In the case of Registration Points managed by entities other than Asseco Data Systems S.A. (external Registration Points), a detailed scope of duties of the Points and their operators may be specified in an additional agreement between external Registration Points and such Points, Certification Practice Statement and the procedures concerning operating of the Registration Points, which are an integral part of the agreement.
2.1. Repositories *Provide the direct URLs to the CA's repositories*	Repository: http://certum.eu/certum/179898.xml	

2.2 Publication of information - RFC 3647 "Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**."		The CPS are structured in accordance with RFC 3647.
2.2 Publication of information - CAA Effective as of 8 September 2017 ... CA's Certificate Policy and/or Certification Practice Statement ... SHALL ... **clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue.**	CPS chapter 4.2.4.	Certum performs CAA (Certification Authority Authorization) records checking when issuing subscribers' certificates Certification Authority Authorization (CAA) Resource Record. Certum accepts the following issue and issuewild CAA records: • certum.pl • certum.eu • yandex.ru
2.2. Publication of information - BR text "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> ***Copy the specific text that is used into the explanation in this row. (in English)***	CPS chapter 1.4	Certum is the member of CA/B Forum and provides its services in accordance with the requirements of the latest published version of: • Baseline Requirements for the Issuance and Management of PubliclyTrusted Certificates, • Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates and • Guidelines For The Issuance And Management Of Extended Validation Certificates. In the event of any inconsistency between this document and the CA/B Forum requirements, the requirements take precedence over this document.

2.2. Publication of information - test websites "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> ***List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.***		https://valid-ctrca.certificates.certum.pl https://revoked-ctrca.certificates.certum.pl https://expired-ctrca.certificates.certum.pl https://valid-cec384ca.certificates.certum.pl https://revoked-cec384ca.certificates.certum.pl https://expired-cec384ca.certificates.certum.pl https://valid-certum-ctnca.certificates.certum.pl/ https://revoked-certum-ctnca.certificates.certum.pl/ https://expired-certum-ctnca.certificates.certum.pl/ https://valid-certum-ctnca2.certificates.certum.pl/ https://revoked-certum-ctnca2.certificates.certum.pl/ https://expired-certum-ctnca2.certificates.certum.pl/
2.3. Time or frequency of publication "The CA SHALL ... **annually** update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. Section 3.3 of Mozilla's Root Store Policy states: "CPs and CPSes MUST be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements. **CAs MUST indicate that this has happened by incrementing the version number and adding a dated changelog entry**, even if no other changes are made to the document." *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	CPS chapter 2.3, 9.12 CP chapter 9	Certum publications below are issued with the following frequency: • the Certification Policy and the Certification Practice Statement – see CPS chapter 9.12, • certificates of the certification authorities functioning within Certum – upon every issuance of new certificates, • the registration authorities certificates – upon every issuance of new certificates, • subscribers' certificates – upon every issuance of new certificates, on subscribers' prior approval, • the Certificate Revocation List – see CPS chapter 4.9.7, • the records of audits carried out by an authorized authority – every time Certum receives them, • supplementary information – upon every updating of it.
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	CPS chapter 2.4	The whole information published by CERTUM in its repository at http://www.certum.eu is accessible for the public. (http://www.certum.eu/certum/cert,aboutus_about_webtrust.xml)

3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CPS chapter 3.2.2. , 3.2.5	The registration authority may collect the data required for identification through publicly available databases, legal entity's authorized representative's personal attendance in the registration authority, or the registration authority representative's presence in person in the legal entity's seat (specified in the application) also, the identity can be authenticated on-line by means of messages exchanged directly with the certification authority or its agent.Where a certificate request contains the name of the organization (O), then this should be interpreted as the person who requests for a certificate is affiliated or authorized to act on behalf of the organization. This means that Certum verifies that the individual who requests for a certificate was an employee organization or its subcontractor at the time of issuance of the certificate and has the right to act on behalf of the organization; the scope of authorization and the period of validity may be regulated by separate legislation or the relying party in the course of verification a digital signature or decryption the received document and is outside the scope of liability of Certum; individual's identity and authorization may be checked by Certum on the basis of available records or database, contact by phone or e-mail to the organization.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CPS chapter 3.1.6	Names that are not owned by a subscriber cannot be used in his/her/its applications. In the event of any question or doubt, the applicant is obliged to attach documents proving their ownership. (Information only about trademarks)
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CPS 3.2.2	If the subject:countryName field is present, then Certum verify the country associated with the Subject using the ccTLD of the requested Domain Name.
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.* ***Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."***	CPS 3.2.2.1	For all SSL certificates, authentication of the Applicant's ownership or control of all requested Domain Name(s) Certum uses one of the following methods: • by uploading file with the specified name to the directory /.well-known/pki-validation of the domain; • by uploading specific metadata to the DNS text record of the domain; • by successfully replying to a challenge response email sent to one or more of the following email addresses: webmaster@domain.com, postmaster@domain.com, admin@domain.com, administrator@domain.com, hostmaster@domain.com. For all SSL certificates containing IP address Certum uses one of the above listed verification methods.
3.2.2.4.1 Validating the Applicant as a Domain Contact For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.	not used	not used

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	not used	not used
3.2.2.4.3 Phone Contact with Domain Contact **CAs SHALL NOT perform validations using this method after May 31, 2019**. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.	not used	not used
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CPS chapter 3.2.2.1	by successfully replying to a challenge response email sent to one or more of the following email addresses: webmaster@domain.com, postmaster@domain.com, admin@domain.com, administrator@domain.com, hostmaster@domain.com.
3.2.2.4.5 Domain Authorization Document "For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates."	not used	not used
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CPS chapter 3.2.2.1	by uploading file with name certum.txt to the directory /.well-known/pki-validation of the domain;
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CPS chapter 3.2.2.1	by uploading specific metadata to the DNS text record of the domain;
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	not used	not used
3.2.2.4.9 Test Certificate **"This method has been retired and MUST NOT be used."**	not used	not used

3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* *This subsection contains major vulnerabilities.* ***If the CA uses this method, then the CA should describe how they are mitigating those vulnerabilities. If not using this method, the CPS should say so.***	not used	not used
3.2.2.4.11 Any Other Method **"This method has been retired and MUST NOT be used."**	not used	not used
3.2.2.4.12 Validating Applicant as a Domain Contact "This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name." If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs*.	not used	not used
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, ***indicate which methods your CA uses*** *and how your CA meets the requirements in this section of the BRs.* **Section 2.2 of Mozilla's root store policy says: "the CA must ensure that the applicant has control over all IP Address(es) referenced in the certificate. This must be done using one or more of the methods documented in section 3.2.2.5 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.5 it is complying with."**	CPS 3.2.2.5	Certum verifies the IP address in the same way as the domains.
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*	CPS 3.1.1.	Certum employs an automated process that prevent the release of certificate with a wildcard character (*) which occurs in the first label position to the left of the top level domain.
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	CPS 3.2.2.	Information Sources e.g. publicly available records of companies/organizations registries. CERTUM is required to request suitable documents from the subscriber, which without any doubts confirm the identity of the legal entity on whose behalf the application is submitted and the private entity that represent it (or submits the application). "

3.2.2.8 CAs MUST check and process CAA records *Indicate how your CA meets the requirements in this section of the BRs.* *Section 2.2 of the BRs states: "**CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."***	CPS chapter 4.2.4	"Certum performs CAA (Certification Authority Authorization) records checking when issuing subscribers' certificates. Certum accepts the following CAA records: • certum.pl • certum.eu • yandex.ru"
3.2.3. Authentication of Individual Identity	CPS chapter 3.2.3	The authentication must prove that data provided in an application concern an existing private entity and the requester is indeed the private entity stated in the application. Procedures and requirements for private entity identity authentication are the same as for legal entities.
3.2.5. Validation of Authority	CPS chapter 3.2.5	Certum verifies that the individual who requests for a certificate was an employee organization or its subcontractor at the time of issuance of the certificate and has the right to act on behalf of the organization; the scope of authorization and the period of validity may be regulated by separate legislation or the relying party in the course of verification a digital signature or decryption the received document and is outside the scope of liability of Certum; individual's identity and authorization may be checked by Certum on the basis of available records or database, contact by phone or e-mail to the organization
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS chapter 3.2.7	Certum may provide interoperation services that allow other entities to be able to interoperate with the Certum by certifying that entities.Accredited entities shall receive certificates for the provision of adequate services. These certificates are issued by Certum Global Services CA and Certum Global Services CA SHA2. Such certificates may be revoked if an annual audit results – carried out by the authorized unit of Certum or other acceptable auditors – show a gross negligence accredited company and which are not remedied within the period specified by the auditor. Cross-certificates are disclosed in WebTrust audit report: https://www.certum.eu/en/cert_aboutus_about_webtrust/
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CPS chapter 4.1.1.	The requester of certificate can be any entity belonging to one of the following categories: • an individual person, which is or will be the subject of certificate, • an authorized representative of the legal person or institution, called an applicant, • an authorized representative of the certification authority certum and ctnDomena domains or an authorized representative of the accredited external authority, • an authorized representative of the Primary Registration Authority or the registration authority. Certum does not issue certificates to entities that reside in countries where the law of Republic of Poland prohibit doing business. EV SSL certificates can only be issued to Private Organizations, Government Entities, Business Entities and NonCommercial Entity subjects. Certum does not issue EV SSL certificates to the natural persons. Suspicius certificate requests idicate by: checking WHOIS, visual check of domain, checking Phishtank, Alexa Top Site etc."

4.1.2. Enrollment Process and Responsibilities	CPS chapter 4.1.2	"All subscribers of certificates and all end users should accept the commitments and guarantees defined in Terms of Use or Subscriber Agreement and undergo the registration process that requires the implementation of the following: • submission of an application which is completed and containing true and correct information; • subscriber generates his/her/its key pair by himself/herself/itself. The generation may also be delegated to CERTUM • in the case of self-generate a key pair subscriber should provide the public key to CERTUM directly or through the registration authority associated with CERTUM, and also prove possession of private key corresponding to public key submitted."
4.2. Certificate application processing	CPS chapter 4.1.2	"An application for registration is submitted to the registration authority or directly to the certification authority by the subscriber and includes the following information: • full name of the institution or the name and surname of the subscriber or certificate administrator, • distinguished name whose structure depends on the subscriber's category (DN) • identifiers: NIP (Tax Identification Number) or REGON (Business Entity Identification Number)/ PESEL (Personal Identification Number) subscriber's postal address (state or province, postal code, city or town, building number and street, fax number), • email address, • the certificate type that the subscriber applies for, • the identifier of certification policy on the basis of which the certificate is to be issued, • the public key that is to be certified. Depending on the content of the certificate and its class, some of the data mentioned above may be optional. "
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.* **Re-use of validation information is limited to 825 days**		For certificates issued on or after March 1, 2018, Certum MAY use the documents and data to verify certificate information provided that Certum obtained these data or documents no more than 825 days prior to issuing the certificate,

4.2.2. Approval or Rejection of Certificate Applications "Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name."	CPS chapter 4.2.2	Proccesing: Every application submitted to the certification authority or submitted to the registration authority, is processed in the following way: • the registration authority operator obtains subscriber's application • the registration authority operator checks whether the subscriber has made a charge for processing an application for a certificate, • the operator verifies data listed in the application, e.g. subscriber's personal data (and checks the proof of private key possession if it exists , • upon the positive verification, the operator confirms (signs) the request; if the original application contains incorrect data, it is rejected or corrected, • basis on the confirmed request a certificate is issued, • the registration authority may also verify other data that are not listed in an application and required by Certum to run a business. Rejection: Certificate issuance denial can occur: • if the subscriber cannot prove his/her rights to the proposed DN, • if there is suspicion or certainty that the subscriber falsified the data or stated false data, • if the subscriber in especially inconvenient manner engaged resources and processingmeans of Certum by submitting number of request clearly in excess of his/her/its needs, • subscriber did not make a payment for issuing a certificate, provided that such payment is provided in the price list of Certum, • from other reasons not specified above.
4.3.1. CA Actions during Certificate Issuance	CPS chapter 4.3.1	Issuance procedure is the following: • any certification request is recorded and verified at the Primary Registration Point, • only persons performing trusted roles have access to operational accounts of the Primary Registration Point. Using the accounts is protected by multi-level authentication and enables the processing of certificate application including the ability to submit an appropriately formatted certificate request to the issuing CA, • a processed certificate applications is sent to certificate issuance server, • if the application contains the request for generating of a key pair, the server charges hardware key generator complying with the requirements of at least FIPS 140 Level 3 with this task, • quality of submitted or generated by a certification authority public keys is tested, • if the procedures are successful, the server issues the certificate and charges hardware security module with signing the certificate; the certificate is stored in certification authority database, • the certification authority prepares an answer containing the issued certificate (if it was issued) and makes it available to the subscriber.

4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	CPS chapter 4.9.1	Certum revokes subscriber's certificate within 24 hours if the following situation occurs: • on each request of the subscriber indicated in the certificate, • subscriber notifies Certum that the original certificate request was not authorized and does not retroactively grant authorization; • when a private key, associated with a public key contained in the certificate or media used for storing it has been compromised, or there is a reason to strongly suspect it would be compromised17; • Certum obtains evidence that the validation of the request was carried out on the basis of incorrect information
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	CPS chapter 4.9.3.2	The certificate belonging to a certification authority or registration authority may be revoked by its issuing authority. Such entity is required to submit request revocation directly to Certum. Certum may also submit Certification Authority's or Registration Authority's certificate revocation request.
4.9.2. Who Can Request Revocation	CPS chapter 4.9.2.	The following entities may submit subscriber's certificate request revocation: • a subscriber who is the owner of a certificate, • an authorized representative of a certification authority (in the case of CERTUM this role is reserved for the security inspector), • a subscriber's requester / payer, for example his/her employer; the subscriber has to be immediately informed about such fact, • a registration authority operator, which may request revocation on behalf of a subscriber or on its own, if it has information justifying certificate revocation.
4.9.3. Procedure for Revocation Request	CPS chapter 4.9.3.1.	•Submission of electronic revocation request authorized by a password, to the certification authority; such revocation is proceeded by subscriber in an unassisted manner. •Submission of electronic revocation request to a certification authority, confirmed with an electronic signature of a registration authority; this method applies to situations when the subscriber has lost both his/her/its private key and its password or revocation request has been submitted by the applicant, an authorized representative of a certification authority or a registration authority, provided that there are sufficient reasons to request such revocation, • The third method involves submission of an authenticated non-electronic request (paper document, fax, phone call, etc) to Primary Certification Authority; authentication of a paper document (including fax) is described at https://www.certum.pl.
4.9.5. Time within which CA Must Process the Revocation Request	CPS chapter 4.9.4.	Certum guarantees maximum 24 hours grace period for revocation request processing.
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	CPS chapter 4.9.7	Every Certificate Revocation List is updated at least once a week if no additional certificate has been revoked within this period. Notwithstanding, the new CRL is published in the repository after every certificate revocation.
4.9.9. On-line Revocation/Status Checking Availability	CPS chapter 4.9.9	Certum provides real-time certificate status verification service. This service is carried out on the basis of OCSP, described in RFC6960.

4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section,* ***including support of GET, update frequency, preventing errounious return of "good" status.***	CPS chapter 4.9.10	Relying parties must check revocation information of a certificate on which they wishes to rely. Otherwise all Certum's warranties becomes void.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CPS chapter 4.9.11	In the case of security breach of private keys (their revelation) of the certification authorities within Certum, the appropriate information is placed immediately in CRL and (optionally) submitted via electronic mail to every subscriber of the certification authority whose private key has been revealed. The information is submitted to every subscriber whose interests may be (directly or indirectly) endangered. Stapling is not supported.
4.10.1. Operational Characteristics	CPS chapter 4.10.1	Information about the status of certificates issued by Certum can be obtained on the Certificate Revocation List (CRL) published on the website Certum, via the LDAP directory service and OCSP services, unless that information is contained in the certificate or the certificate status verification services are the objects of an agreement between subscriber and Asseco Data Systems S.A.
4.10.2. Service Availability	CPS chapter 4.10.2	Certificate status verification services are available in the regime 24/7
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	CPS chapter 5.1	Network computer system, operator's terminals and information resources of Certum are located in the dedicated area, physically protected against unauthorized access, destruction or disruption to its operation. These locations are monitored. Every entry and exit is recorded in the system logs.
5.2.2. Number of Individuals Required per Task	CPS chapter 5.2.2	Keys – for the needs of certificate and CRL signing – generation process is the operation requiring particular attention. The generation requires presence of persons, acting as: • security inspector, • hardware security module operator, • shared secret holder, • commentator, Any other operation and role, described within Certum, may be performed by a single person, assigned for such an operation or role.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS chapter 5.3.1.	A person performing his / her duties, arising from the role held in the certification authority or the registration office must meet the following requirements: • has graduated from at least the secondary school, • has signed a work contract or other civil agreement describing his/her role in the system and corresponding responsibilities, • has been subjected to required training on the range of obligations and tasks, associated with his/her position, • has been trained in the field of personal data protection, • has signed an agreement containing clause concerning sensitive (from the point of view of Certum security) information protection and confidentiality and privacy of subscriber's data, • does not perform tasks which may lead to a conflict of interests between a certification authority and a registration authority acting on behalf of it.

5.3.3. Training Requirements and Procedures	CPS chapter 5.3.3.	Personnel performing roles and tasks arising from the employment in Certum or its registration authority have to complete following trainings: • regulations of Certification Practice Statement, regulations of Certification Policy, • regulations of procedures and documentation related with acted role, • procedures and security controls employed by a certification authority and a registration authority, • system software of a certification authority and a registration authority, • responsibilities arising from roles and tasks performed in the system, • procedures executed upon system malfunction or disruption of certification authority operations.
5.3.4. Retraining Frequency and Requirements	CPS chapter 5.3.4.	Trainings have to be repeated or supplemented always in situation when significant modification to Certum or its registration authority operation is executed.
5.3.7. Independent Contractor Controls	CPS chapter 5.3.7.	Contract personnel or consultants may perform trusted roles, they are subject to the same requirements applicable in the case of workers employed in Certum. Contract personnel are subjected to the same verification procedure as employees of Certum and its registration authority and Additionally, contract personnel, when performing their task at Certum seat or its registration authority have to be escorted by Certum or the registration authority employee.
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	CPS chapter 5.4.1.	Every activity, critical for Certum security, is recorded in event logs and archived. Archives might be encrypted and stored on unrewritable media type to prevent it from modification or forgery. Certum event logs store records of every activity generated by any software component within the system. Such entries are divided into three separate categories: • system entries – record contains information about client's request and server's response (or vice-versa) on the level of network protocol (for example http, https, tcp, etc); Subjects to recordings are: host or server IP address, executed operation (for example: search, edit, write, etc) and its output (for example, amount of entries to database), • errors – record contains information about errors on the level of network protocols and on the level of application modules, • audits – record contains information associated with certification services, for example: registration and certificate request, rekey request, certificate acceptance, certificate and CRL issuance etc.
5.4.3. Retention Period for Audit Logs	CPS chapter 5.4.3.	Retention period for audit log are at least 7 years.
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	CPS chapter 5.4.8	Certification Practice Statement requires the certification authority issuing certificates the Primary Registration Authority and affiliated Registration Points to perform vulnerability assessment analysis of every internal procedures, applications and information system. Scan of vulnerabilities are held 4 times a year. Requirements for analysis may be also determined by an external institution, authorized to carry out Certum audit.
5.5.2. Retention Period for Archive	CPS chpater 5.5.2	Certum retain all documentation (in paper and electronic form) relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven years after any certificate based on that documentation ceases to be valid.,

5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	CPS chapter 5.7.1	Incidents handling and responding to threats are regulated by Certum Business Continuity Plan. At least once a year Certum tests the effectiveness of the procedures covered by the Business Continuity Plan.
6.1.1. Key Pair Generation	CPS chapter 6.1.1.	Certification authorities key pair are generated in accordance with the accepted by Certum procedure for key pair generation. Actions executed while performing key pair generation are recorded, dated and signed by each person present during the generation. The records are retained for the needs of audits and common system reviews.
6.1.2. Private Key Delivery to Subscriber	CPS chapter 6.1.2.	Subscriber's key pair is generated by himself/herself/itself or may be generated centrally by a certification authority inside a token (e.g. an electronic identity card) In the case of keys generation by Certum keys are delivered (together with a token) to the subscriber personally or by means of registered mail; data for the card activation (including PIN/PUK) or key decryption (password) are submitted separately from the media containing the key pair; the issued cards are personalized and registered by the certification authority.
6.1.5. Key Sizes	CPS chapter 6.1.5	Size of keys deployed in most of the Certum's certification authorities is 2048 bits excluding Certum Trusted Network CA 2 which has 4096-bit keys and Certum Trusted Network CA EC authority key which has 521-bit in length but encrypted with ECDH_P521 algorithm The key length in certificates used by the Primary Registration Authority operators and subscribers are defined by the user (2048 bit or more).
6.1.6. Public Key Parameters Generation and Quality Checking	CPS chapter 6.1.6	Certum generates keys in accordance with FIPS 186. If key pair is generated by subscriber, Certum always validates the quality of public keys presented by subscribers before the issuance of subscriber's certificate. He/she/it is required to verify: • ability to execute encryption and decryption operation, including electronic signature creation and its verification, • key generation process, which should be based on strong random cryptographic number generators – physical sources of white noise, if possible, • immunity to known attacks (applies to RSA cryptographic algorithm). Additionally, every certification authority, upon reception or generation (on subscriber's demand) of a public key, subjects it to appropriate verification test on compliance with restrictions enforced by the Certification Practice Statement.
6.1.7. Key Usage Purposes	CPS chapter 6.1.7.	Allowed key usage purposes are described in keyUsage field of standard extension of a certificate complying with X.509 v3. This field has not to be obligatorily verified by the subscribers' application managing the certificates. Usage of every bit of keyUsage field has to comply with the RFC 5280. Certificates used for both signature creation and encryption may be issued solely to subscribers.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS chapter 6.2. 6.2.1	Every subscriber, Certum's certification authority operator and the Primary Registration Authority operator generates and stores his/her/its private key employing a credible system preventing from private key loss, revelation, modification or unauthorized access. Hardware security modules employed by a certification authority and a registration authority comply with the requirements of FIPS 140-2 Level 3 or higher standard. In the case of subscriber's using hardware key protection, it is recommended to comply with FIPS 140-2 Level 2 or higher.

6.2.5. Private Key Archival	CPS chapter 6.2.5.	Private keys of all Certum's certification authorities are archived only by Certum. Private keys of certification authorities used for electronic signature creation are archived for at least 5 years after their usage termination in cryptographic operation. The same requirement applies to public key certificate corresponding to private key after its expiration or revocation. Private keys of certification authorities used in key agreement operations have to be archived after expiry of the validity date of the associated certificate or upon its revocation for the period at least 5 years. Archived keys have to be available for 25 years; for the first 15 years they must be accessible on-line. Certum does not archives copies of registration authority's and subscriber's private keys.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS chapter 6.2.6	Operation of entering of a private key into a cryptographic module is carried out in the following cases: • in the case of creation of backup copies of private keys stored in a cryptographic module, it may be occasionally necessary (e.g. in the case of the module corruption or malfunction) to enter a key pair into a different security module, • it is necessary to transfer a private key from the operational module used for standard operations by the entity to another module; the situation may occur in the case of the module defection or necessity of its destruction
6.2.7. Private Key Storage on Cryptographic Module	CPS chapter 6.2.7	Hardware security modules employed by Certum's certification authorities comply with the requirements of FIPS 140-2 Level 3 or higher standard. Regardless of the form of the private key's storage, the key is not accessible from outside the cryptographic module for unauthorized entities.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	CPS chapter 6.3.2	The maximum validity period for website authentication certificates is 825 days
6.5.1. Specific Computer Security Technical Requirements **The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.** *Indicate how your CA meets the requirements of this section.*	CPS chapter 6.5.1	Computers operated within Certum's certification authorities and in their associated components are equipped with the following securitycontrols: • mandatory authenticated registration on the level of operating system and application(in the case of significant importance, e.g. due to the role performed in the system), • discretionary access control, • possibility of conducting security audit, • computers are accessible only by personnel, performing trusted roles in Certum, • enforcement of duty segregation, arising from the role performed in the system, • identification and authentication of roles and personnel performing these roles, • cryptographic protection of information exchange session and protection of databases, • archive of history of operation carried out on the computer and data required by audits, • a secure path allowing credible identification and authentication of roles and personnel performing these roles, • key restoration methods (only in the case of hardware security modules) and application and operating system, • monitoring and alerting means in the case of unauthorized computer resources access.

7.1. Certificate profile **CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG.** *Indicate how your CA meets the requirements of this section.*	CPS chapter 7.1	Certum supports the following certificate basic fields: • Version: third version (X.509 v.3) of certificate format, • SerialNumber: certificate serial number, unique within certification authority domain (Certum generates non-sequential certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from aCSPRNG); • SignatureAlgorithm: identifier of the algorithm applied by a certification authority issuing certificates, • Issuer: distinguished name (DN) of a certification authority, • Validity: validity period, described by the beginning date (notBefore) and the ending date (notAfter) of the certificate validity period, • Subject: distinguished name (DN) of the subscriber that is the subject of the certificate, • SubjectPublicKeyInfo: value of a public key along with the identifier of the algorithm associated with the key, • Signature: the sign generated and encoded according to RFC 5280.
7.1.1. Version Number(s)	CPS chapter 7.1.1.	All certificates belonging to Certum are issued in accordance with Version 3 (X.509 v.3).
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CPS chapter 7.1.2.	The extensions values are created in accordance with RFC 5280. Function of every extension is defined by the standard value of the corresponding object identifier (OBJECT IDENTIFIER).
7.1.2.1 Root CA Certificate	CPS chapter 7.1.2.	The extensions values are created in accordance with RFC 5280
7.1.2.2 Subordinate CA Certificate	CPS chapter 7.1.2.	The extensions values are created in accordance with RFC 5280

7.1.2.3 Subscriber Certificate	CPS chapter 7.1.2.	The extensions values are created in accordance with RFC 5280
7.1.2.4 All Certificates	CPS chapter 7.1.2.	The extensions values are created in accordance with RFC 5280
7.1.2.5 Application of RFC 5280	CPS chapter 7.1.2	The extensions values are created in accordance with RFC 5280. Function of every extension is defined by the standard value of the corresponding object identifier (OBJECT IDENTIFIER).
7.1.3. Algorithm Object Identifiers	CPS chapter 7.1.3	RSA algorithm, in combination with SHA-1, SHA-384, SHA-256 or SHA-512 cryptographic hash is used.
7.1.4. Name Forms	CPS chapter 7.1.4	Certificates issued by Certum contain the name of the issuer and name of the subject, which are developed in accordance with the principles described in the CPS and CP.
7.1.4.1 Issuer Information	CPS chapter 7.1	Common Name (CN) = Proper root certificate name Organization (O) = Unizeto Sp. z o.o. (within certum) or Unizeto Technologies S.A. (within ctnDomena) Organization Unit (OU) = Certum Certification Authority (only within ctnDomena) Country=PL

7.1.4.2 Subject Information - Subscriber Certificates Section 7.1.4.2.1 states: Certificate Field: extensions:**subjectAltName** Required/Optional: Required Contents: **This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.** Wildcard FQDNs are permitted. Section 7.1.4.2.2 states: Certificate Field: subject:commonName (OID 2.5.4.3) Required/Optional: Deprecated (Discouraged, but not prohibited) Contents: **If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension** (see Section 7.1.4.2.1).	CPS chapter 7.1	Distinguished names comply with the X.501 requirements. Values of all attributes of these fields are optional, except for the following fields: emailAddress (in the case of individual's certificates), organizationName (in the case of non-Repudiation and CA certificates), subjectAltName (in the case of server certificates: contain all domain names or IP addresses), commonName (in the case of server certificates: contain a single IP address or a domain name that is one of the values contained in the certificate's subjectAltName extension), unstructured {Address or Name} (in the case of VPN certificates) which are mandatory
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CPS chapter 7.1.4	Certificates issued by Certum contain the name of the issuer and name of the subject, which are developed in accordance with the principles described in the chapter 3.1.1.
7.1.5. Name Constraints ***Indicate your CA's understanding of section 5.3 of Mozilla's root store policy, and requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section of the BRs.*** ***"All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's root program:*** ***MUST be audited in accordance with Mozilla's Root Store Policy. ...*** ***MUST be publicly disclosed in the CCADB by the CA that has their certificate included in Mozilla's root program. The CA with a certificate included in Mozilla's root program MUST disclose this information within a week of certificate creation, and before any such subordinate CA is allowed to issue certificates. ..."***	CPS chapter 7.1.5.	Certum may include name constraints in the nameConstraints field when appropriate.
7.1.6. Certificate Policy Object Identifier	CPS chapter 7.1.6.	Certification Policy contains information of the policy Information type (identifier, electronic address) about a certification policy, applied by the issuing authority – this extension is not critical.
7.1.6.1 Reserved Certificate Policy Identifiers	CPS chapter 7.1.6.	Certificate policy object identifiers (OIDs) are listed in 1.2 and 1.3.1.2
7.1.6.2 Root CA Certificates	CPS chapter 7.1.6.	Certificate policy object identifiers (OIDs) are listed in 1.2 and 1.3.1.2
7.1.6.3 Subordinate CA Certificates	CPS chapter 7.1.6.	Certificate policy object identifiers (OIDs) are listed in 1.2 and 1.3.1.2
7.1.6.4 Subscriber Certificates	CPS chapter 7.1.6.	Certificate policy object identifiers (OIDs) are listed in 1.2 and 1.3.1.2

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CPS chapter 8	The audit mainly regards a data processing and key management procedures. It also concerns all certification authorities belonging to the certification path of primary certification authority Certum CA and Certum Trusted Network CA, the Primary Registration Authority, and other elements of public key infrastructure, e.g. OCSP server. Certum audit may be carried out by internal units of Asseco Data Systems S.A. (internal audit) and organizational units independent from Asseco Data Systems S.A. (external audit). In both cases, an audit is carried out on request of and under supervision of a security inspector
8.1. Frequency or circumstances of assessment **The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.** For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	CPS chapter 8.1.	Carried out at least once a year
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	CPS chapter 8.2.	An external audit is carried out by an authorized and independent from Certum domestic institution or the institution with a representation in Poland. Such an institution should: • hire employees who possess appropriate technical knowledge (with supplied documents proving it) concerning public key infrastructure, information security techniques and devices, and security auditing, • be a registered, well-known and respected organization or society.` An internal audit is carried out by designated unit, operating within Asseco Data Systems S.A. structure.
8.4. Topics covered by assessment	CPS chapter 8.4.	External and internal audits are carried out in accordance with the rules specified by American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) Web Trust Principles and Criteria for Certification Authorities. The scope of Web Trust audit includes: • physical security of Certum, • procedures of subscribers' identity verification, • certification services and procedures of the services delivery, • security of software and network access, • security of Certum personnel, • system journals and system monitoring procedures, • backup copy creation and their recovery, • archive procedures, • records of configuration parameters changes of CERTUM , records of software and devices inspection and service.
8.6. Communication of results	CPS chapter 8.6.	Audit records (as detailed as possible) and the auditor's general opinion are published in the repository upon every audit.

Also indicate your understanding and compliance with section 3 of Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements		
8.7. Self-Audits	CPS chapter 8.0 and 8.2.	Certum audit may be carried out by internal units of Asseco Data Systems S.A. (internal audit). An internal audit is carried out by designated unit, operating within Asseco Data Systems S.A. structure.

9.6.1. CA Representations and Warranties	CPS chapter 9.6 and 9.6.1.	Certum ensures that: • at the time of issuance, Certum implemented a procedure for verifying that the Subscriber either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the certificate's subject field and subjectAltName extension, • at the time of issuance, Certum implemented a procedure for verifying that the Subscriber Representative is authorized to request the certificate on behalf of the Subscriber, • at the time of issuance, Certum implemented a procedure for verifying the accuracy of all of the information contained in the certificate (with the exception of the subject: organizationalUnitName attribute, • at the time of issuance, Certum implemented a procedure for reducing the likelihood that the information contained in the certificate's organizationalUnitName attribute would be misleading, • when issuing the certificate, if the certificate contains subject identity information, Certum implemented a procedure to verify the identity of the subscriber, • Certum will revoke the certificate for any of the reasons specified in this CPS. • its commercial activity is based on reliable devices and software creating a system that fulfils requirements stated in FIPS 140-2 Security Requirements for Cryptographic Modules
9.6.3. Subscriber Representations and Warranties	CPS chapter 9.6.3	The Primary Registration Authority and every Registration Point operating within Certum or bound by an agreement with Certum ensures that: • its commercial activity is based on reliable devices and software, recommended by Certum, • its activity and services are in accordance with the law and do not violate copyrights and licensed third parties rights, • it makes reasonable efforts to secure that subscriber's identification data set in Certum database are correct, and this information is updated in the moment of the data confirmation, • confirmed subscriber's information, later sent to a certification authority for including it to a certificate, is precise, • it does not contribute intentionally to mistakes or inaccuracy in information contained in a certificate, • its services are in accordance with broadly accepted norms (de jure and de facto): X.509, PKCS#10, PKCS#7, PKCS#12,
9.8. Limitations of liability	CPS chapter 9.8	If damages are the fault of Certum or of the parties that Asseco Data Systems S.A. made agreement with in such a way that the fault is transferred to Certum,
9.9.1. Indemnification by CAs	CPS chapter 9.9.1	Subscriber liability results from the obligations and warranties stated in CPS. The liability conditions are governed by an agreement with Asseco Data Systems S.A..

9.16.3. Severability	CPS chapter 9.16.3	If particular parts of the present document or the agreements made on the grounds of it are regarded as violating the law in force or against the law, a court can order to respect the remaining (i.e. in accordance with the law) part of Certification Practice Statement or agreements already made, unless questioned parts are not significant from the point of view of exchange (e.g. commercial transaction) that the parties agreed on